

INPI

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

09/88958

PCT/FR00/00188

REC'D 14 APR 2000

WIPO

PCT

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

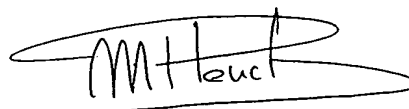
Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 06 AVR. 2000

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA
RÈGLE 17.1.a) OU b)



Martine PLANCHE

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE

26 bis, rue de Saint Petersburg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

Best Available Copy


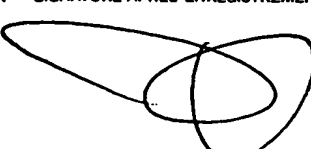
This Page Blank (uspto)

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

REQUÊTE EN DÉLIVRANCE

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

<p>DATE DE REMISE DES PIÈCES 23 MARS 1999</p> <p>N° D'ENREGISTREMENT NATIONAL 99 03770</p> <p>DÉPARTEMENT DE DÉPÔT</p> <p>DATE DE DÉPÔT 23 MARS 1999 N. P. I. RENNES</p>		<p>1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE</p> <p>Patrice VIDON Cabinet Patrice VIDON Immeuble Germanium 80 avenue des Buttes de Coësmes 35700 RENNES</p>									
<p>2 DEMANDE Nature du titre de propriété industrielle</p> <p><input checked="" type="checkbox"/> brevet d'invention <input type="checkbox"/> demande divisionnaire</p> <p><input type="checkbox"/> certificat d'utilité <input type="checkbox"/> transformation d'une demande de brevet européen</p> <p style="text-align: center;">demande initiale</p> <p><input type="checkbox"/> brevet d'invention <input type="checkbox"/> certificat d'utilité n°</p> <p>Établissement du rapport de recherche <input checked="" type="checkbox"/> différé <input type="checkbox"/> immédiat</p> <p>Le demandeur, personne physique, requiert le paiement échelonné de la redevance <input type="checkbox"/> oui <input type="checkbox"/> non</p> <p>Titre de l'invention (200 caractères maximum)</p> <p style="text-align: center;">Procédé, système, dispositif pour diminuer la charge de travail pendant une session destinée à prouver l'authenticité d'une entité et/ou l'origine et l'intégrité d'un message.</p>		<p>n° du pouvoir permanent références du correspondant 5343bis téléphone 02.99.38.23.00</p>									
<p>3 DEMANDEUR (S) n° SIREN</p> <p>Nom et prénoms (souligner le nom patronymique) ou dénomination</p> <p>1. FRANCE TELECOM</p> <p>2. TELEDIFFUSION DE France</p> <p>3. MATH RIZK</p> <p>Nationalité (s) Française</p> <p>Adresse (s) complète (s)</p> <p>1. 6 place d'Alleray 75015 PARIS</p> <p>2. 10, rue d'Oradour-sur-Glane 75732 PARIS Cédex 15</p>		<p>code APE-NAF</p> <p>Forme juridique</p> <p>Société Anonyme</p> <p>Société Anonyme</p> <p>SPRL (Société de droit belge)</p> <p>Pays</p> <p>France (1,2)</p> <p>Belgique (3)</p>									
<p>4 INVENTEUR (S) Les inventeurs sont les demandeurs <input type="checkbox"/> oui <input checked="" type="checkbox"/> non Si la réponse est non, fournir une désignation séparée</p>											
<p>5 RÉDUCTION DU TAUX DES REDEVANCES <input type="checkbox"/> requise pour la 1ère fois <input type="checkbox"/> requise antérieurement au dépôt : joindre copie de la décision d'admission</p>											
<p>6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE</p> <table style="width:100%;"> <tr> <td>pays d'origine</td> <td>numéro</td> <td>date de dépôt</td> <td>nature de la demande</td> </tr> <tr> <td>FRANCE</td> <td>9901065</td> <td>27/01/99</td> <td></td> </tr> </table>				pays d'origine	numéro	date de dépôt	nature de la demande	FRANCE	9901065	27/01/99	
pays d'origine	numéro	date de dépôt	nature de la demande								
FRANCE	9901065	27/01/99									
<p>7 DIVISIONS antérieures à la présente demande n° date n° date</p>											
<p>8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (nom et qualité du signataire)</p> <p>P. VIDON (CPI 92-1250)</p>		<p>SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI</p> <p> </p>									

DÉSIGNATION DE L'INVENTEUR

(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

DEPARTEMENT DES BREVETS

26bis, rue de Saint-Petersbourg

75800 Paris Cédex 08

Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

N° D'ENREGISTREMENT NATIONAL

99 03 770

TITRE DE L'INVENTION :

Procédé, système, dispositif pour diminuer la charge de travail pendant une session destinée à prouver l'authenticité d'une entité et/ou l'origine et l'intégrité d'un message.

LE(S) SOUSSIGNÉ(S)

Patrice VIDON

Cabinet Patrice VIDON

Immeuble Germanium

80 avenue des Buttes de Coësmes

35700 RENNES

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

M. Louis GUILLOU

16 rue de l'Ise

35230 BOURGBARRE

FRANCE

M. Jean-Jacques QUISQUATER

3 avenue des canards

B-1640 Rhode Saint Genèse

BELGIQUE

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

le 23 mars 1999

P. VIDON (CPI 92-1250)

DOCUMENT COMPORTANT DES MODIFICATIONS

PAGE(S) DE LA DESCRIPTION OU DES REVENDEICATIONS OU PLANCHE(S) DE DESSIN			R.M.*	DATE DE LA CORRESPONDANCE	TAMPON DATEUR DU CORRECTEUR
Modifiée(s)	Supprimée(s)	Ajoutée(s)			
67			NON	01/06/99	02 DEC. AJP

Un changement apporté à la rédaction des revendications d'origine, sauf si celui-ci découle des dispositions de l'article R.612-36 du Code de la Propriété Intellectuelle, est signalé par la mention « R.M. » (revendications modifiées).

Procédé, système, dispositif pour diminuer la charge de travail pendant une session destinée à prouver l'authenticité d'une entité et/ou l'origine et l'intégrité d'un message.

La présente invention concerne les procédés, les systèmes ainsi que les dispositifs destinés à prouver l'authenticité d'une entité et/ou l'origine et l'intégrité d'un message.

Le brevet EP 0 311 470 B1 dont les inventeurs sont Louis Guillou et Jean-Jacques Quisquater décrit un tel procédé. On y fera ci-après référence en le désignant par les termes : « brevet GQ » ou « procédé GQ ».

Selon le procédé GQ, une entité appelée « autorité de confiance » attribue une identité à chaque entité appelée « témoin » et en calcule la signature RSA; durant un processus de personnalisation, l'autorité de confiance donne identité et signature au témoin. Par la suite, le témoin proclame : « *Voici mon identité ; j'en connais la signature RSA.* » Le témoin prouve sans la révéler qu'il connaît la signature RSA de son identité. Grâce à la clé publique de vérification RSA distribuée par l'autorité de confiance, une entité appelée « contrôleur » vérifie sans en prendre connaissance que la signature RSA correspond à l'identité proclamée. Les mécanismes utilisant le procédé GQ se déroulent « sans transfert de connaissance ». Selon le procédé GQ, le témoin ne connaît pas la clé privée RSA avec laquelle l'autorité de confiance signe un grand nombre d'identités. La sécurité du procédé GQ est au mieux équivalente à la connaissance de la signature RSA de l'identité. Il y a équivalence lorsque l'exposant public de vérification RSA est un nombre premier.

Le procédé GQ met en œuvre des calculs modulo des nombres de 512 bits ou davantage. Ces calculs concernent des nombres ayant sensiblement la même taille élevés à des puissances de l'ordre de $2^{16} + 1$. Or les infrastructures microélectroniques existantes, notamment dans le domaine des cartes bancaires, font usage de microprocesseurs auto-programmables

monolithiques dépourvus de coprocesseurs arithmétiques. La charge de travail liée aux multiples opérations arithmétiques impliquées par des procédés tels que le procédé GQ, entraîne des temps de calcul qui dans certains cas s'avèrent pénalisant pour les consommateurs utilisant des cartes bancaires pour acquitter leurs achats. Il est rappelé ici, qu'en cherchant à accroître la sécurité des cartes de paiement, les autorités bancaires posent un problème particulièrement délicat à résoudre. En effet, il faut traiter deux questions apparemment contradictoires : augmenter la sécurité en utilisant des clés de plus en plus longues et distinctes pour chaque carte tout en évitant que la charge de travail n'entraîne des temps de calcul prohibitifs pour les utilisateurs. Ce problème prend un relief particulier dans la mesure où, en outre, il convient de tenir compte de l'infrastructure en place et des composants microprocesseurs existants.

L'invention a pour objet d'apporter une solution à ce problème tout en renforçant la sécurité. Plus particulièrement, l'invention concerne un procédé pour diminuer la charge de travail pendant une session destinée à prouver à un contrôleur,

- l'authenticité d'une entité et/ou
- l'origine et l'intégrité d'un message m .

Procédé

Le procédé selon l'invention, met en œuvre les trois entités ci-après définies.

I. Une première entité, appelée témoin, dispose des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$. Le témoin dispose aussi

* des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ..., représentant des clés privées QA, QB, \dots

* des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

* des exposants publics de vérification v_x, v_y, \dots

Les clés privées et les clés publiques sont liées par des relations du type :

$$GA \cdot QA^{v_x} \bmod n \equiv 1 \text{ ou } GA \equiv QA^{v_x} \bmod n$$

Les exposants publics de vérification v_x, v_y, \dots sont utilisés par le témoin pour calculer des engagements R en effectuant des opérations du type :

$$R_i \equiv r_i^{v_x} \bmod p_i$$

ou r_i est un aléa tel que $0 < r_i < p_i$.

Ainsi, selon le nouveau procédé, les rôles de témoin et d'autorité de confiance fusionnent. Chaque témoin utilise la factorisation $p_1, p_2, \dots (p_1, \dots)$ de son propre module public n . De sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n . L'usage de la factorisation du module n réduit significativement la charge de travail du témoin. Par rapport au procédé GQ, et a fortiori par rapport à d'autres procédés tel que le procédé RSA de signature, le procédé selon l'invention permet de substantielles économies de calcul, en particulier pour l'authentification.

II. Le procédé selon l'invention met en œuvre une deuxième entité pilote dudit témoin. Cette entité pilote est appelée

* démonstrateur dans le cas de la preuve de l'authenticité d'une entité ou de l'authenticité d'un message,

* signataire dans les cas de la preuve de l'origine et de l'intégrité d'un message.

On verra ci-après quel est son rôle.

III. La troisième entité, appelée contrôleur, vérifie l'authentification ou l'origine et l'intégrité d'un message.

Selon l'invention, le témoin reçoit de la deuxième entité pilote ou du contrôleur un ou plusieurs défis d tel que $0 \leq d \leq v_x - 1$ et calcule à partir de ce défi une ou plusieurs réponses D en effectuant des opérations du type :

$$D_i \equiv r_i \cdot QA_i^d \pmod{p_i}$$

ou r_i est un aléa tel que $0 < r_i < p_i$

On constatera ici, de même que précédemment, que le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacune des réponses D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

Le contrôleur reçoit, selon le cas, une ou plusieurs réponses D . Il calcule, à partir desdites réponses D , les engagements R' en effectuant des opérations du type :

$$R'_i \equiv GA^d \cdot D^{r_i} \pmod{n}$$

ou du type :

$$R'_i \cdot GA^d \equiv D^{r_i} \pmod{n}$$

Le contrôleur peut alors vérifier que les triplets $\{R', d, D\}$ sont cohérents.

Dans le cas général qui vient d'être exposé, il y a plusieurs exposants de vérifications vx , vy , On va maintenant exposer l'invention dans le cas où l'exposant de vérification v est unique.

Cas où l'exposant de vérification v est unique

De même que précédemment, le procédé selon l'invention met en œuvre trois entités :

I. Une première entité, appelée témoin, dispose des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$.

Le témoin dispose aussi

* des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ..., représentant des clés privées QA, QB, \dots

* des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

* de l'exposant public de vérification v

Dans ce cas comme dans le précédent, il est prévu plusieurs paires de clés

référéncées **A, B, ...**

Les paires de clés privées et publiques sont liées par des relations du type :

$$\mathbf{GA.QA^v \bmod n \equiv 1 \text{ ou } \mathbf{GA \equiv QA^v \bmod n}}$$

L'exposant public unique de vérification **v** est utilisé par le témoin pour calculer des engagements **R**. A cet effet :

- il effectue des opérations du type :

$$\mathbf{R_i \equiv r_i^v \bmod p_i}$$

où **r_i** est un entier, tiré au hasard, associé au nombre premier **p_i**, tel que $0 < r_i < p_i$, appartenant à au moins une collection d'aléas **{r₁, r₂, r₃, ...}**,

- puis il applique la méthode dite des restes chinois, (on décrira ci-après la méthode des restes chinois qui est connue en soi).

Il y a autant d'engagements **R** que de collections d'aléas **{r₁, r₂, r₃, ...}**,

Bien entendu, dans ce cas comme dans le cas général précédent, le nombre d'opérations arithmétiques modulo **p_i** à effectuer pour calculer chacun des **R_i** pour chacun des **p_i** est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo **n**.

II. La deuxième entité pilote dudit témoin est appelée :

* démonstrateur dans le cas de la preuve de l'authenticité d'une entité ou de l'authenticité d'un message,

* signataire dans les cas de la preuve de l'origine et de l'intégrité d'un message,

III. La troisième entité, appelée contrôleur, vérifie l'authentification ou l'origine et l'intégrité d'un message.

Plus particulièrement, dans le cas de cette variante de réalisation le témoin reçoit de la deuxième entité ou du contrôleur, des collections de défis **d** **{dA, dB, ...}** tels que $0 \leq dA \leq v - 1$. Le nombre des collections de défis **d** est égal au nombre d'engagements **R**. Chaque collection **{dA, dB, ...}** comprend un nombre de défis égal au nombre de paires de clés.

Le témoin calcule à partir de chacune desdites collections de défis **{dA, dB,**

...} des réponses **D**. A cet effet :

- il effectue des opérations du type :

$$D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \bmod p_i$$

- puis il applique la méthode des restes chinois.

5 Il y a autant de réponses **D** que d'engagements **R** et de défis **d**.

Il convient de souligner, ici aussi, que le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

10 Le contrôleur reçoit une réponse **D**. Il calcule à partir de cette réponse un engagement **R'** en effectuant des opérations du type :

$$R' \equiv GA^{dA} \cdot GB^{dB} \cdot \dots D' \bmod n$$

ou du type :

$$R' \cdot GA^{dA} \cdot GB^{dB} \cdot \dots \equiv D' \bmod n$$

15 Le contrôleur vérifie que les triplets $\{R', d, D\}$ sont cohérents.

Ainsi, grâce à la présente invention, le témoin qui proclame : « *Voici une clé publique de vérification (v, n) et une clé publique GA ; je connais la factorisation de n et la clé privée QA* » prouve sans la révéler qu'il connaît la clé privée QA . Le contrôleur vérifie la clé privée QA sans en prendre connaissance. Les mécanismes se déroulent « sans transfert de connaissance ». On le verra ci-après, que le procédé selon l'invention autorise certaines paires de clés telles que la connaissance de la clé privée QA est équivalente à la connaissance de la factorisation du module n .

20 On va maintenant exposer les variantes de réalisation de l'invention concernant :

- le cas d'une authentification d'entité,
- le cas d'une authentification de message,
- le cas d'une signature numérique de message.

Cas d'une authentification d'entité

Cas où l'exposant de vérification v est unique.

Dans le cas de cette variante de réalisation particulière, la session est destinée à prouver à un contrôleur l'authenticité d'une entité.

Comme dans le cas général, la session met en œuvre trois entités.

- 5 I. Une première entité, appelée témoin, dispose des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$,

Le témoin dispose aussi :

- 10 * des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$,
 ..., représentant des clés privées QA, QB, \dots
 * des clés publiques GA, GB, \dots ayant respectivement pour
 composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$
 * de l'exposant public de vérification v

Les paires de clés privées et publiques sont liées par des relations du type :

15
$$GA \cdot QA' \bmod n \equiv 1 \text{ ou } GA \equiv QA' \bmod n$$

II. La deuxième entité, pilote dudit témoin, est appelée démonstrateur.

III. La troisième entité, appelée contrôleur, vérifie l'authentification.

Pour prouver l'authenticité d'une entité, le témoin, le démonstrateur et le contrôleur exécutent les étapes suivantes :

- 20 • **étape 1. engagement R du témoin :**

A chaque appel, le témoin tire au hasard et en privé au moins une collection de nombres entiers $\{r_1, r_2, r_3, \dots\}$, telle que, pour chaque facteur premier p_i , chaque collection comporte un aléa r_i positif et plus petit que p_i ,

Pour chaque facteur premier p_i , le témoin élève chaque aléa r_i à la
 25 puissance v ième modulo p_i

$$R_i \equiv r_i^v \bmod p_i$$

On notera que le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

Puis, le témoin établit chaque engagement R modulo n selon la méthode des restes chinois.

Il y a autant d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$,

• **étape 2. défi d destiné au témoin :**

5 Le démonstrateur transmet tout ou partie de chaque engagement R au contrôleur.

Le contrôleur, après avoir reçu tout ou partie de chaque engagement R , produit au moins une collection de défis d $\{dA, dB, \dots\}$ tels que $0 \leq dA \leq v - 1$. Le nombre des collections de défis d est égal au nombre d'engagements R . Chaque collection $\{dA, dB, \dots\}$ comprend un nombre de défis égal au nombre de paires de clés.

10

• **étape 3. réponse du témoin au défi d :**

Le témoin calcule des réponses D à partir des collections de défis d $\{dA, dB, \dots\}$ reçues du contrôleur. A cet effet :

15

il effectue des opérations du type :

$$D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \mod p_i$$

puis, il applique la méthode des restes chinois.

Le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

20

Il y a autant de réponses D calculées par le témoin que d'engagements R et de défis d .

• **étape 4. données destinées au contrôleur :**

Le démonstrateur transmet au contrôleur chaque réponse D .

25

• **étape 5. vérification par le contrôleur :**

Le contrôleur calcule à partir de chaque réponse D un engagement R' en effectuant des opérations du type :

$$R' \equiv GA^{dA} \cdot GB^{dB} \cdot \dots D' \mod n$$

ou du type :

$$R' \cdot GA^{dA} \cdot GB^{dB} \cdot \dots \equiv D' \pmod{n}$$

Le contrôleur vérifie que chaque engagement reconstruit R' reproduit tout ou partie de chaque engagement R transmis à l'étape 2 par le démonstrateur.

5

Cas d'une authentification de message

cas où l'exposant de vérification v est unique.

Dans le cas de cette variante de réalisation particulière, la session est destinée à prouver à un contrôleur l'authenticité d'un message m .

Comme dans le cas général, la session met en œuvre trois entités.

10

I. Une première entité, appelée témoin, dispose des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$,

Le témoin dispose aussi :

15

- * des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ..., représentant des clés privées QA, QB, \dots

- * des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

- * de l'exposant public de vérification v

Les paires de clés privées et publiques sont liées par des relations du type :

20

$$GA \cdot QA' \pmod{n} \equiv 1 \text{ ou } GA \equiv QA' \pmod{n}$$

II. Une deuxième entité, pilote du témoin, est appelée démonstrateur.

III. Une troisième entité, appelée contrôleur, vérifie l'authenticité d'un message.

Pour prouver l'authenticité d'un message le témoin, le démonstrateur et le contrôleur exécutent les étapes suivantes :

25

• étape 1. engagement R du témoin :

A chaque appel, le témoin tire au hasard et en privé au moins une collection de nombres entiers $\{r_1, r_2, r_3, \dots\}$, telle que pour chaque facteur premier p_i , chaque collection comporte un aléa r_i positif et plus petit que p_i .

Pour chaque facteur premier p_i , le témoin élève chaque aléa r_i à la puissance v ième modulo p_i

$$R_i \equiv r_i^v \text{ mod } p_i$$

(de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n)

Puis, le témoin établit chaque engagement R modulo n selon la méthode des restes chinois.

Il y a autant d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$,

• étape 2. défi d destiné au témoin :

Le démonstrateur applique une fonction de hachage f ayant comme arguments le message m et chaque engagement R pour obtenir un jeton T .

Le démonstrateur transmet le jeton T au contrôleur,

Le contrôleur, après avoir reçu le jeton T , produit au moins une collection de défis d $\{dA, dB, \dots\}$ tels que $0 \leq dA \leq v - 1$. Le nombre des collections de défis d est égal au nombre d'engagements R . Chaque collection $\{dA, dB, \dots\}$ comprend un nombre de défis égal au nombre de paires de clés.

• étape 3. réponse du témoin au défi d :

Le témoin calcule les réponses D à partir des collections de défis d $\{dA, dB, \dots\}$ reçues du contrôleur. A cet effet,

il effectue des opérations du type :

$$D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \text{ mod } p_i$$

puis, il applique la méthode des restes chinois.

Le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

Il y a autant de réponses D calculées par le témoin que d'engagements R et de défis d .

• étape 4. données destinées au contrôleur :

Le démonstrateur transmet au contrôleur chaque réponse **D**.

• **étape 5. vérification par le contrôleur :**

Le contrôleur calcule à partir de chaque réponse **D** un engagement **R'** en effectuant des opérations du type :

$$5 \quad R' \equiv GA^{dA} \cdot GB^{dB} \cdot \dots D' \bmod n$$

ou du type :

$$R' \cdot GA^{dA} \cdot GB^{dB} \cdot \dots \equiv D' \bmod n$$

10 Le contrôleur applique la fonction de hachage **f** ayant comme arguments le message **m** et chaque engagement reconstruit **R'** pour reconstruire le jeton **T'**.

Le contrôleur vérifie que le jeton **T'** est identique au jeton **T** transmis à l'étape 2 par le démonstrateur.

Cas d'une signature numérique de message

Cas où l'exposant de vérification **v est unique.**

15 Dans le cas de cette variante de réalisation particulière, la session est destinée à prouver à un contrôleur la signature numérique d'un message **m**. Comme dans le cas général, la session met en œuvre trois entités.

I. Une première entité appelée témoin dispose des facteurs premiers **p₁, p₂, ... (p_i, ...)** (**i** étant supérieur ou égal à 2) d'un module public **n** tel que **n = p₁ · p₂ · p₃ · ...**.

20 Le témoin dispose aussi

* des composantes **QA₁, QA₂, ... (QA_i, ...)**, et **QB₁, QB₂, ... (QB_i, ...)**, ..., représentant des clés privées **QA, QB, ...**

25 * des clés publiques **GA, GB, ...** ayant respectivement pour composantes **GA₁, GA₂, ... (GA_i, ...)** et **GB₁, GB₂, ... (GB_i, ...)**

* de l'exposant public de vérification **v**.

Les paires de clés privées et publiques sont liées par des relations du type :

$$GA \cdot QA' \bmod n \equiv 1 \text{ ou } GA \equiv QA' \bmod n$$

II. Une deuxième entité, pilote dudit témoin, est appelée signataire.

III. Une troisième entité, appelée contrôleur, vérifie la signature du message **m**.

Pour prouver la signature d'un message le témoin, le démonstrateur et le contrôleur exécutent les étapes suivantes :

5 • **étape 1. engagement R du témoin :**

A chaque appel, le témoin tire au hasard et en privé au moins une collection de nombres entiers $\{r_1, r_2, r_3, \dots\}$, telle que, pour chaque facteur premier p_i , chaque collection comporte un aléa r_i positif et plus petit que p_i .

10 Pour chaque facteur premier p_i , le témoin élève chaque aléa r_i à la puissance v ième modulo p_i

$$R_i \equiv r_i^v \pmod{p_i}$$

(de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n)

15 Puis, le témoin établit chaque engagement **R** modulo n selon la méthode des restes chinois.

Il y a autant d'engagements **R** que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$.

 • **étape 2. défi d destiné au témoin :**

20 Le signataire applique une fonction de hachage **f** ayant comme arguments le message **m** et chaque engagement **R** pour obtenir au moins une collection de défis **d** $\{dA, dB, \dots\}$ tels que $0 \leq dA \leq v - 1$. Le nombre des collections de défis **d** est égal au nombre d'engagements **R**, chaque collection $\{dA, dB, \dots\}$ comprend un nombre de défis égal au nombre de paires de clés.

Le signataire transmet les collections de défis **d** au témoin.

25 • **étape 3. réponse du témoin au défi d :**

Le témoin calcule des réponses **D** à partir desdites collections de défis **d** $\{dA, dB, \dots\}$ reçues du contrôleur. A cet effet, il effectue des opérations du type :

$$D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \pmod{p_i}$$

(de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n)

puis, il applique la méthode des restes chinois.

5 Il y a autant de réponses D calculées par le témoin que d'engagements R et de défis d .

Le témoin transmet les réponses D au signataire et/ou au contrôleur.

• **étape 4. données destinées au contrôleur :**

Le signataire transmet un message signé au contrôleur comprenant :

- 10
- le message m ,
 - les collections de défis d ou les engagements R ,
 - chaque réponse D

• **étape 5. vérification par le contrôleur :**

Cas où le contrôleur reçoit la collection des défis d ,

15 Dans le cas où le contrôleur reçoit la collection des défis d et des réponses D , ledit contrôleur calcule à partir de chaque réponse D un engagement R' en effectuant des opérations du type :

$$R' \equiv GA^{d_A} \cdot GB^{d_B} \cdot \dots D' \pmod{n}$$

ou du type :

20

$$R' \cdot GA^{d_A} \cdot GB^{d_B} \cdot \dots \equiv D' \pmod{n}$$

Le contrôleur applique la fonction de hachage f ayant comme arguments le message m et chaque engagement reconstruit R' pour reconstruire chaque défi d' .

25 Le contrôleur vérifie que chaque défi d' reconstruit est identique au défi d figurant dans le message signé.

Cas où le contrôleur reçoit la collection des engagements R

Dans le cas où le contrôleur reçoit la collection des engagements R et des réponses D , ledit contrôleur applique la fonction de hachage f ayant comme arguments le message m et chaque engagement R pour reconstruire chaque

défi d' .

Le contrôleur reconstruit alors la collection des engagements R' en effectuant des opération du type

$$R' \equiv GA^{d'A} \cdot GB^{d'B} \cdot \dots D' \text{ mod } n$$

ou du type :

$$R' \cdot GA^{d'A} \cdot GB^{d'B} \cdot \dots \equiv D' \text{ mod } n$$

Le contrôleur vérifie que chaque engagement R' reconstruit est identique à l'engagement R figurant dans le message signé.

**Paire de clés selon la présente invention conférant une sécurité
équivalente à la connaissance de la clé privée Q**

La paire de clés GA, QA, \dots n'a plus de raison d'être systématiquement déduite de l'identité du témoin, comme dans le cas du procédé GQ.

Selon une variante de réalisation, un grand nombre de témoins utilisent le même ensemble de clés publiques très courtes $GA, GB, GC, GD \dots$ par exemple, 4, 9, 25 et 49.

Dans le cas de la variante de réalisation ci-après exposée les composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ... des clés privées QA, QB, \dots sont des nombres tirés au hasard à raison d'une composante QA_i, QB_i, \dots pour chacun desdits facteurs premiers p_i . Lesdites clés privées QA, QB , peuvent être calculées à partir desdites composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ... par la méthode des restes chinois.

Les clés publiques GA, GB, \dots sont calculées en effectuant des opérations du type :

$$GA_i \equiv QA_i' \text{ mod } p_i$$

puis en appliquant la méthode des restes chinois pour établir GA tel que

$$GA \equiv QA' \text{ mod } n$$

ou bien tel que

$$GA \cdot QA' \text{ mod } n \equiv 1$$

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer pour

calculer chacun des GA_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

De préférence l'exposant public de vérification v est un nombre premier. Dans ce cas la paire de clés GA, QA confère une sécurité équivalente à la connaissance de la clé privée QA .

Paire de clés selon la présente invention conférant une sécurité équivalente à la connaissance de la factorisation de n

De préférence, l'exposant public de vérification v est du type

$$v = a^k$$

où k est un paramètre de sécurité plus grand que 1.

De préférence, également l'exposant public de vérification v est du type

$$v = 2^k$$

où k est un paramètre de sécurité plus grand que 1.

Dans ce cas, la clé publique GA est un carré gA^2 inférieur à n choisi de sorte que les deux équations

$$x^2 \equiv gA \pmod{n} \quad \text{et} \quad x^2 \equiv -gA \pmod{n}$$

n'ont pas de solution en x dans l'anneau des entiers modulo n .

Les composantes $QA_1, QA_2, \dots (QA_i, \dots)$ de la clé privée QA sont alors telles que :

$$GA \equiv QA_i^{2 \exp(k)} \pmod{p_i}$$

ou bien telles que :

$$GA \cdot QA_i^{2 \exp(k)} \pmod{p_i} \equiv 1$$

On les obtient en extrayant la k ième racine carrée de GA dans le corps de Galois $CG(p_i)$,

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des QA_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

On démontre que la paire de clés GA, QA confère une sécurité équivalente à la connaissance de la factorisation de n .

De préférence, pour extraire la k ième racine carrée de GA dans le corps de Galois $CG(p_i)$, on utilise les méthodes suivantes :

- dans le cas où le facteur premier p_i est congru à 3 modulo 4, on applique notamment un algorithme du type :

$$x = (p+1)/4 ; y \equiv x^k \text{ mod } (p-1) ; z = y ; QA_i \equiv GA^z \text{ mod } p_i$$

- dans le cas où le facteur premier p_i est congru à 1 modulo 4, on emploie les suites de Lucas.

Système

La présente invention concerne également un système permettant de mettre en œuvre le procédé ci-dessus exposé.

Le système selon l'invention permet de diminuer la charge de travail pendant une session destinée à prouver à un serveur contrôleur,

- l'authenticité d'une entité et/ou
- l'origine et l'intégrité d'un message m .

Le système met en œuvre trois entités :

I. Une première entité, appelée dispositif témoin, contenue notamment dans un objet nomade se présente par exemple sous la forme d'une carte bancaire à microprocesseur.

Le dispositif témoin dispose d'une première zone mémoire contenant des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$.

Le dispositif témoin dispose aussi d'une deuxième zone mémoire contenant :

* des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ..., représentant des clés privées QA, QB, \dots

* des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

* des exposants publics de vérification vx, vy, \dots

lesdites clés privées et clés publiques étant liées par des relations du type :

$$GA \cdot QA^x \bmod n \equiv 1 \text{ ou } GA \equiv QA^x \bmod n$$

Le dispositif témoin comporte aussi des premiers moyens de calcul pour calculer des engagements R en effectuant des opérations du type :

$$R_i \equiv r_i^x \bmod p_i$$

5 ou r_i est un aléa tel que $0 < r_i < p_i$,

II. Le système met en œuvre une deuxième entité, appelée dispositif pilote dudit dispositif témoin. Elle peut être contenue notamment dans ledit objet nomade. Le dispositif pilote est plus précisément appelé :

10 * dispositif démonstrateur dans le cas de la preuve de l'authenticité d'une entité ou de l'authenticité d'un message,

* dispositif de signature dans les cas de la preuve de l'origine et de l'intégrité d'un message,

15 III. Le système met en œuvre une troisième entité, appelée dispositif contrôleur, se présentant notamment sous la forme d'un terminal et/ou d'un serveur distant connecté à un réseau de communication informatique. Le dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique au dispositif témoin. Le dispositif contrôleur vérifie l'authentification ou l'origine et l'intégrité d'un message.

20 Le dispositif témoin reçoit du dispositif pilote ou du dispositif contrôleur un ou plusieurs défis d tel que $0 \leq d \leq vx - 1$. Il comporte des deuxièmes moyens de calcul pour calculer à partir des défis d une ou plusieurs réponses D en effectuant des opérations du type :

$$D_i \equiv r_i \cdot QA_i^d \bmod p_i$$

25 ou r_i est un aléa tel que $0 < r_i < p_i$

(de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer par lesdits deuxièmes moyens de calcul pour calculer chacune des réponses D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n)

Le dispositif contrôleur, reçoit une ou plusieurs réponses **D**. Il comporte des troisièmes moyens de calcul pour calculer à partir desdites réponses **D** des engagements **R'** en effectuant des opérations du type :

$$R'_i \equiv GA^d \cdot D^{v_i} \pmod{n}$$

5 ou du type :

$$R'_i \cdot GA^d \equiv D^{v_i} \pmod{n}$$

Le dispositif contrôleur comporte des quatrièmes moyens de calcul pour vérifier que les triplets **{R', d, D}** sont cohérents.

Cas où l'exposant de vérification *v* est unique

10 De même que précédemment, le système selon l'invention met en œuvre trois entités.

I. Une première entité, appelée dispositif témoin, contenue notamment dans un objet nomade se présentant par exemple sous la forme d'une carte bancaire à microprocesseur.

15 Le dispositif témoin dispose d'une première zone mémoire contenant des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$,

Le dispositif témoin dispose aussi d'une deuxième zone mémoire contenant :

20 * des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ..., représentant des clés privées **QA, QB, ...**

* des clés publiques **GA, GB, ...** ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$,

* un exposant public de vérification **v**.

25 Les paires de clés privées et publiques sont liées par des relations du type :

$$GA \cdot QA^v \pmod{n} \equiv 1 \text{ ou } GA \equiv QA^v \pmod{n}$$

Le dispositif témoin comporte aussi des premiers moyens de calcul pour calculer des engagements **R**. A cet effet,

• il effectue des opérations du type :

$$R_i \equiv r_i \cdot v \pmod{p_i}$$

où r_i est un entier, tiré au hasard, associé au nombre premier p_i , tel que $0 < r_i < p_i$, appartenant à au moins une collection d'aléas $\{r_1, r_2, r_3, \dots\}$,

• puis, il applique la méthode des restes chinois.

5 Il y a autant d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$,

Le nombre d'opérations arithmétiques modulo p_i à effectuer par lesdits premiers moyens de calcul pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

10 **II.** La deuxième entité, appelée dispositif pilote dudit dispositif témoin, peut être contenue notamment dans ledit objet nomade. Le dispositif pilote est appelé :

* dispositif démonstrateur dans le cas de la preuve de l'authenticité d'une entité ou de l'authenticité d'un message,

15 * dispositif de signature dans les cas de la preuve de l'origine et de l'intégrité d'un message,

III. La troisième entité, appelée dispositif contrôleur, se présente notamment sous la forme d'un terminal et/ou d'un serveur distant connecté à un réseau de communication informatique. Le dispositif contrôleur
20 comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique audit dispositif témoin. Le dispositif contrôleur vérifie l'authentification ou l'origine et l'intégrité d'un message,

Plus particulièrement, dans le cas de cette variante de réalisation, le
25 dispositif témoin reçoit du dispositif pilote ou du dispositif contrôleur, des collections de défis d $\{dA, dB, \dots\}$ tels que $0 \leq dA \leq v - 1$. Le nombre des collections de défis d est égal au nombre d'engagements R . Chaque collection $\{dA, dB, \dots\}$ comprend un nombre de défis égal au nombre de paires de clés.

Le dispositif témoin comporte des deuxièmes moyens de calcul pour calculer à partir de chacune desdites collections de défis $\{dA, dB, \dots\}$ des réponses D . A cet effet,

- il effectue des opérations du type :

$$5 \quad D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \bmod p_i$$

- puis, il applique la méthode des restes chinois.

Il y a autant de réponses D que d'engagements R et de défis d .

Il convient de souligner, ici aussi, que le nombre d'opérations arithmétiques modulo p_i à effectuer par lesdits deuxièmes moyens de calcul pour calculer chacun des D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

Le dispositif contrôleur reçoit une ou plusieurs réponses D . Il comporte des troisièmes moyens de calcul pour calculer à partir desdites réponses D un engagement R' en effectuant des opérations du type :

$$15 \quad R' \equiv GA^{dA} \cdot GB^{dB} \cdot \dots D' \bmod n$$

ou du type :

$$R' \cdot GA^{dA} \cdot GB^{dB} \cdot \dots \equiv D' \bmod n$$

Le dispositif contrôleur comporte des quatrièmes moyens de calcul pour vérifier que les triplets $\{R', d, D\}$ sont cohérents.

20 On va maintenant exposer les variantes de réalisation du système selon l'invention concernant :

- le cas d'une authentification d'entité,
- le cas d'une authentification de message,
- le cas d'une signature numérique de message.

25 **Cas d'une authentification d'entité**

Cas où l'exposant de vérification v est unique.

Dans le cas de cette variante de réalisation particulière, la session est destinée à prouver à un contrôleur l'authenticité d'une entité.

Comme dans le cas général, la session met en œuvre trois entités du

système selon l'invention.

I. Une première entité, appelée dispositif témoin, contenue notamment dans un objet nomade se présentant par exemple sous la forme d'une carte bancaire à microprocesseur.

5 Le dispositif témoin dispose d'une première zone mémoire contenant des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$. Le dispositif témoin dispose aussi d'une deuxième zone mémoire contenant :

10 * des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$,
..., représentant des clés privées QA, QB, \dots

* des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

* un exposant public de vérification v .

Les paires de clés privées et publiques sont liées par des relations du type :

15 $GA \cdot QA' \bmod n \equiv 1$ ou $GA \equiv QA' \bmod n$

II. La deuxième entité, appelée dispositif démonstrateur dudit dispositif témoin, peut être contenue notamment dans ledit objet nomade.

20 **III.** Une troisième entité, appelée dispositif contrôleur, se présente sous la forme d'un terminal et/ou d'un serveur distant connecté à un réseau de communication informatique. Le dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique audit dispositif témoin,

Pour prouver l'authenticité d'une entité, ledit dispositif témoin, ledit dispositif démonstrateur et ledit dispositif contrôleur exécutent les étapes
25 suivantes :

• **étape 1. engagement R du dispositif témoin :**

Le dispositif témoin comporte des premiers moyens de calcul pour tirer au hasard et en privé, à chaque appel, au moins une collection de nombres entiers $\{r_1, r_2, r_3, \dots\}$, telle que, pour chaque facteur premier p_i , chaque

collection comporte un aléa r_i positif et plus petit que p_i .

Le dispositif témoin comporte des deuxièmes moyens de calcul pour élever chaque aléa r_i à la puissance v ième modulo p_i , pour chaque facteur premier p_i ,

$$5 \quad R_i \equiv r_i^v \pmod{p_i}$$

On notera que le nombre d'opérations arithmétiques modulo p_i à effectuer par les deuxièmes moyens de calcul pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

10 Puis, lesdits deuxièmes moyens de calcul du dispositif témoin établissent chaque engagement R modulo n selon la méthode des restes chinois.

Il y a autant d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$,

• **étape 2. défi d destiné au dispositif témoin :**

15 Le dispositif démonstrateur comporte des moyens de transmission pour transmettre tout ou partie de chaque engagement R au dispositif contrôleur.

Le dispositif contrôleur comporte des troisièmes moyens de calcul pour calculer, après avoir reçu tout ou partie de chaque engagement R , au moins une collection de défis d $\{dA, dB, \dots\}$ tels que $0 \leq dA \leq v - 1$. Le nombre des collections de défis d est égal au nombre d'engagements R . Chaque
20 collection $\{dA, dB, \dots\}$ comprend un nombre de défis égal au nombre de paires de clés.

• **étape 3. réponse du dispositif témoin au défi d :**

Le dispositif témoin comporte des quatrièmes moyens de calcul pour calculer des réponses D , à partir desdites collections de défis d $\{dA, dB, \dots\}$ reçues du dispositif contrôleur. A cet effet,

25 il effectue des opérations du type :

$$D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \pmod{p_i}$$

puis, il applique la méthode des restes chinois.

Le nombre d'opérations arithmétiques modulo p_i à effectuer par les

quatrièmes moyens de calcul pour calculer chacun des D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

Il y a autant de réponses D calculées par le témoin que d'engagements R et de défis d .

• **étape 4. données destinées au dispositif contrôleur :**

Le démonstrateur comporte des moyens de transmission pour transmettre au dispositif contrôleur chaque réponse D .

• **étape 5. vérification par le dispositif contrôleur :**

Le dispositif contrôleur comporte des cinquièmes moyens de calcul pour calculer à partir de chaque réponse D un engagement R' en effectuant des opérations du type :

$$R' \equiv GA^{dA} \cdot GB^{dB} \cdot \dots D' \text{ mod } n$$

ou du type :

$$R' \cdot GA^{dA} \cdot GB^{dB} \cdot \dots \equiv D' \text{ mod } n$$

Le dispositif contrôleur comporte des sixièmes moyens de calcul pour comparer et vérifier que chaque engagement reconstruit R' reproduit tout ou partie de chaque engagement R transmis à l'étape 2 par le dispositif démonstrateur.

Cas d'une authentification de message

Cas où l'exposant de vérification v est unique.

Dans le cas de cette variante de réalisation particulière, la session est destinée à prouver à un contrôleur l'authenticité d'un message m .

Comme dans le cas général, la session met en œuvre trois entités du système.

I. Une première entité, appelée dispositif témoin, contenue notamment dans un objet nomade se présente par exemple sous la forme d'une carte bancaire à microprocesseur.

Le dispositif témoin dispose d'une première zone mémoire contenant des

facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$. Le dispositif témoin dispose aussi d'une deuxième zone mémoire contenant

* des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$,
5 ..., représentant des clés privées QA, QB, \dots

* des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

* un exposant public de vérification v .

Les paires de clés privées et publiques sont liées par des relations du type :

$$10 \quad GA \cdot QA^v \bmod n \equiv 1 \text{ ou } GA \equiv QA^v \bmod n$$

II. Une deuxième entité, appelée dispositif démonstrateur dudit dispositif témoin, peut être contenue notamment dans ledit objet nomade.

III. Une troisième entité, appelée dispositif contrôleur, se présente sous la forme d'un terminal et/ou d'un serveur distant connecté à un réseau de
15 communication informatique. Le dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique audit dispositif témoin.

Pour prouver l'authenticité d'un message ledit dispositif témoin, ledit dispositif démonstrateur et ledit dispositif contrôleur exécutent les étapes
20 suivantes :

• **étape 1. engagement R du dispositif témoin :**

Le dispositif témoin comporte des premiers moyens de calcul pour tirer au hasard et en privé, à chaque appel, au moins une collection de nombres entiers $\{r_1, r_2, r_3, \dots\}$, telle que pour chaque facteur premier p_i , chaque
25 collection comporte un aléa r_i positif et plus petit que p_i .

Le dispositif témoin comporte des deuxième moyens de calcul pour élever chaque aléa r_i à la puissance v ième modulo p_i , pour chaque facteur premier p_i ,

$$R_i \equiv r_i^v \bmod p_i$$

Le nombre d'opérations arithmétiques modulo p_i à effectuer par les deuxièmes moyens de calcul pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

5 Puis, lesdits deuxièmes moyens de calcul dudit dispositif témoin établissent chaque engagement R modulo n selon la méthode des restes chinois.

Il y a autant d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$.

• **étape 2. défi d destiné au dispositif témoin :**

10 Le dispositif démonstrateur comporte des premiers moyens de calcul pour calculer un jeton T , en appliquant une fonction de hachage f ayant comme arguments le message m et chaque engagement R .

Le dispositif démonstrateur comporte des moyens de transmission pour transmettre le jeton T au dispositif contrôleur.

15 Le dispositif contrôleur comporte des troisièmes moyens de calcul pour calculer, après avoir reçu le jeton T , au moins une collection de défis d $\{dA, dB, \dots\}$ tels que $0 \leq dA \leq v - 1$. Le nombre des collections de défis d est égal au nombre d'engagements R . Chaque collection $\{dA, dB, \dots\}$ comprend un nombre de défis égal au nombre de paires de clés.

• **étape 3. réponse du dispositif témoin au défi d :**

20 Le dispositif témoin comporte des quatrièmes moyens de calcul pour calculer des réponses D , à partir desdites collections de défis d $\{dA, dB, \dots\}$ reçues du dispositif contrôleur. A cet effet, il effectue des opérations du type :

$$D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \bmod p_i$$

25 puis, il appliquant la méthode des restes chinois.

Le nombre d'opérations arithmétiques modulo p_i à effectuer par les quatrièmes moyens de calcul pour calculer chacun des D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

Il y a autant de réponses **D** calculées par le témoin que d'engagements **R** et de défis **d**.

• **étape 4. données destinées au dispositif contrôleur :**

Le démonstrateur comporte des moyens de transmission pour transmettre
5 au dispositif contrôleur chaque réponse **D**.

• **étape 5. vérification par le dispositif contrôleur :**

Le dispositif contrôleur comporte des cinquièmes moyens de calcul pour
calculer à partir de chaque réponse **D** un engagement **R'** en effectuant des
opérations du type :

$$10 \quad R' \equiv GA^{dA} \cdot GB^{dB} \cdot \dots D' \bmod n$$

ou du type :

$$R' \cdot GA^{dA} \cdot GB^{dB} \cdot \dots \equiv D' \bmod n$$

Le dispositif contrôleur comporte des sixièmes moyens de calcul pour
calculer, en appliquant la fonction de hachage **f** ayant comme arguments le
15 message **m** et chaque engagement **R'**, le jeton **T'**.

Le dispositif contrôleur comporte des septièmes moyens de calcul pour
comparer et vérifier que le jeton **T'** est identique au jeton **T** transmis à
l'étape 2 par le dispositif démonstrateur.

Cas d'une signature numérique de message

Cas où l'exposant de vérification **v est unique.**

Dans le cas de cette variante de réalisation particulière, la session est
destinée à prouver à un contrôleur la signature numérique d'un message **m**.
Comme dans le cas général, la session met en œuvre trois entités du
système :

25 **I.** Une première entité, appelée dispositif témoin, contenues notamment
dans un objet nomade se présente par exemple sous la forme d'une carte
bancaire à microprocesseur.

Le dispositif témoin comporte une première zone mémoire contenant des
facteurs premiers **p₁, p₂, ... (p_i, ...)** (**i** étant supérieur ou égal à 2) d'un

module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$.

Le dispositif témoin comporte également une deuxième zone mémoire contenant :

* des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$,
5 ..., représentant des clés privées QA, QB, \dots

* des clés publiques GA, GB, \dots ayant respectivement pour
composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

* un exposant publique de vérification v .

Les paires de clés privées et publiques sont liées par des relations du type :

$$GA \cdot QA^v \bmod n \equiv 1 \text{ ou } GA \equiv QA^v \bmod n$$

II. Une deuxième entité, pouvant être contenue notamment dans ledit objet
nomade, est appelée dispositif de signature.

III. Une troisième entité, appelée dispositif contrôleur se présente sous la
forme d'un terminal et/ou d'un serveur distant connecté à un réseau de
communication informatique. Le dispositif contrôleur comporte des moyens
de connexion pour le connecter électriquement, électromagnétiquement,
optiquement ou de manière acoustique au dispositif témoin.

Pour prouver la signature d'un message, ledit dispositif témoin, ledit
dispositif démonstrateur et ledit dispositif contrôleur exécutent les étapes
suivantes :

• **étape 1. engagement R du témoin :**

Le dispositif témoin comporte des premiers moyens de calcul pour tirer au
hasard et en privé, à chaque appel, au moins une collection de nombres
entiers $\{r_1, r_2, r_3, \dots\}$, telle que pour chaque facteur premier p_i , chaque
collection comporte un aléa r_i positif et plus petit que p_i .

Le dispositif témoin comporte des deuxièmes moyens de calcul pour élever
chaque aléa r_i à la puissance v ième modulo p_i , pour chaque facteur
premier p_i ,

$$R_i \equiv r_i^v \bmod p_i$$

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer par les deuxièmes moyens de calcul pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

5 Puis, lesdits deuxièmes moyens de calcul du dispositif témoin établissent chaque engagement R modulo n selon la méthode des restes chinois.

Il y a autant d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$,

• **étape 2. défi d destiné au dispositif témoin :**

10 Le dispositif de signature comporte des troisièmes moyens de calcul pour calculer, en appliquant une fonction de hachage f ayant comme arguments le message m et chaque engagement R , au moins une collection de défis d $\{dA, dB, \dots\}$ tels que $0 \leq dA \leq v - 1$. Le nombre des collections de défis d est égal au nombre d'engagements R . Chaque collection $\{dA, dB, \dots\}$ comprend un nombre de défis égal au nombre de paires de clés.

15 Le dispositif de signature transmet les collections de défis d au dispositif témoin,

• **étape 3. réponse du dispositif témoin au défi d :**

20 Le dispositif témoin comporte des quatrièmes moyens de calcul pour calculer des réponses D , à partir desdites collections de défis d $\{dA, dB, \dots\}$ reçues du dispositif contrôleur. A cet effet, il effectue des opérations du type :

$$D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \bmod p_i$$

puis, il applique la méthode des restes chinois.

25 Le nombre d'opérations arithmétiques modulo p_i à effectuer par les quatrièmes moyens de calcul pour calculer chacun des D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

Il y a autant de réponses D calculées par le témoin que d'engagements R et de défis d .

Le dispositif témoin comporte des moyens de transmission pour transmettre les réponses **D** au dispositif de signature et/ou au dispositif contrôleur.

• **étape 4. données destinées au dispositif contrôleur :**

Le dispositif de signature transmet au dispositif contrôleur un message signé comprenant :

- le message **m**,
- les collections de défis **d** ou les engagements **R**,
- chaque réponse **D**

• **étape 5. vérification par le dispositif contrôleur :**

Cas où le dispositif contrôleur reçoit la collection des défis d,

Dans le cas où le dispositif contrôleur reçoit les collections des défis **d** et des réponses **D**, ledit dispositif contrôleur comporte des cinquièmes moyens de calcul pour calculer à partir de chaque réponse **D** un engagement **R'** en effectuant des opérations du type :

$$R' \equiv GA^{d_A} \cdot GB^{d_B} \cdot \dots D' \text{ mod } n$$

ou du type :

$$R' \cdot GA^{d_A} \cdot GB^{d_B} \cdot \dots \equiv D' \text{ mod } n$$

Le dispositif contrôleur comporte des sixièmes moyens de calcul pour calculer chaque défi **d'**, en appliquant la fonction de hachage **f** ayant comme arguments le message **m** et chaque engagement reconstruit **R'**.

Le dispositif contrôleur comporte des septièmes moyens de calcul pour comparer et vérifier que chaque défi **d'** est identique au défi **d** figurant dans le message signé.

Cas où le dispositif contrôleur reçoit la collection des engagements R

Dans le cas où le dispositif contrôleur reçoit la collection des engagements **R** et des réponses **D**, ledit dispositif contrôleur comporte des cinquièmes moyens de calcul pour calculer chaque défi **d'**, en appliquant la fonction de hachage **f** ayant comme arguments le message **m** et chaque engagement **R**.

Le dispositif contrôleur comporte des sixièmes moyens de calcul pour

calculer alors la collection des engagements R' en effectuant des opérations du type

$$R' \equiv GA^{d'A} \cdot GB^{d'B} \cdot \dots D^v \text{ mod } n$$

ou du type :

$$5 \quad R' \cdot GA^{d'A} \cdot GB^{d'B} \cdot \dots \equiv D^v \text{ mod } n$$

Le dispositif contrôleur comporte des septièmes moyens de calcul pour comparer et vérifier que chaque engagement R' reconstruit est identique à l'engagement R figurant dans le message signé.

Paire de clés conférant une sécurité équivalente à la connaissance de la clé privée Q

10

Dans le cas de la variante de réalisation ci-après exposée les composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ... des clés privées QA, QB, \dots sont des nombres tirés au hasard à raison d'une composante QA_i, QB_i, \dots pour chacun desdits facteurs premiers p_i , lesdites clés privées QA, QB , pouvant être calculées à partir desdites composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ... par la méthode des restes chinois.

15

Dans le cas de cette variante, le dispositif témoin comporte des huitièmes moyens de calcul pour calculer lesdites clés publiques GA, GB, \dots ,

• en effectuant des opérations du type :

20

$$GA_i \equiv QA_i^v \text{ mod } p_i$$

• puis en appliquant la méthode des restes chinois pour établir GA tel que

$$GA \equiv QA^v \text{ mod } n$$

ou bien tel que

$$GA \cdot QA^v \text{ mod } n \equiv 1$$

25

Le nombre d'opérations arithmétiques modulo p_i à effectuer par les huitièmes moyens de calcul dudit dispositif témoin pour calculer chacun des GA_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

De préférence dans ce cas, l'exposant public de vérification v est un

nombre premier. Il en résulte que la paire de clés GA, QA confère une sécurité équivalente à la connaissance de la clé privée QA.

Paire de clés conférant une sécurité équivalente à la connaissance de la factorisation de n

5 De préférence, l'exposant public de vérification v est du type

$$v = a^k$$

où k est un paramètre de sécurité plus grand que 1.

De préférence également, l'exposant public de vérification v est du type

$$v = 2^k$$

10 où k est un paramètre de sécurité plus grand que 1,

Dans ce cas, la clé publique GA est un carré gA^2 inférieur à n choisi de sorte que les deux équations

$$x^2 \equiv gA \pmod{n} \quad \text{et} \quad x^2 \equiv -gA \pmod{n}$$

n'ont pas de solution en x dans l'anneau des entiers modulo n .

15 Le dispositif témoin comporte des neuvièmes moyens de calcul pour calculer les dites composantes $QA_1, QA_2, \dots (QA_i, \dots)$ de la clé privée QA en appliquant des formules telles que :

$$GA \equiv QA_i^{2 \exp(k)} \pmod{p_i}$$

ou bien telles que :

20
$$GA \cdot QA_i^{2 \exp(k)} \pmod{p_i} \equiv 1$$

et en extrayant la k ième racine carrée de GA dans le corps de Galois $CG(p_i)$.

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer par les neuvièmes moyens de calcul du dispositif témoin pour calculer chacun des QA_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

On démontre que la paire de clés GA, QA confère une sécurité équivalente à la connaissance de la factorisation de n .

De préférence, pour extraire la k ième racine carrée de GA dans le corps de

Galois $CG(p_i)$, on utilise les méthodes suivantes :

- dans le cas où le facteur premier p_i est congru à 3 modulo 4, les neuvièmes moyens de calcul du dispositif témoin appliquent notamment un algorithme du type :

$$x = (p+1)/4 ; y \equiv x^k \bmod (p-1) ; z = y ; QA_i \equiv GA^z \bmod p_i$$

- dans le cas où le facteur premier p_i est congru à 1 modulo 4, les neuvièmes moyens de calcul du dispositif témoin appliquent notamment un algorithme basé sur les suites de Lucas.

Objet nomade. Carte bancaire

La présente invention concerne également un objet nomade permettant de mettre en œuvre le procédé ci-dessus exposé.

L'objet nomade selon l'invention se présente, par exemple, sous la forme d'une carte bancaire à microprocesseur. Il permet de diminuer la charge de travail pendant une session destinée à prouver à un serveur contrôleur,

- l'authenticité d'une entité et/ou
- l'origine et l'intégrité d'un message m ,

L'objet nomade fait intervenir trois entités :

I. Une première entité, appelée dispositif témoin, est contenue dans ledit objet nomade. Le dispositif témoin dispose d'une première zone mémoire contenant des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$. Le dispositif témoin dispose aussi d'une deuxième zone mémoire contenant :

* des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ..., représentant des clés privées QA, QB, \dots

* des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

* des exposants publics de vérification vx, vy, \dots

Les clés privées et les clés publiques sont liées par des relations du type :

$$GA \cdot QA^{vx} \bmod n \equiv 1 \text{ ou } GA \equiv QA^{vy} \bmod n$$

Le dispositif témoin comporte aussi des premiers moyens de calcul pour calculer des engagements R en effectuant des opérations du type :

$$R_i \equiv r_i^{v_x} \bmod p_i$$

ou r_i est un aléa tel que $0 < r_i < p_i$.

5 Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer par lesdits premiers moyens de calcul pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

10 II. Une deuxième entité est appelée dispositif pilote dudit dispositif témoin. Elle peut être également contenue dans ledit objet nomade. Le dispositif pilote est appelé :

* dispositif démonstrateur dans le cas de la preuve de l'authenticité d'une entité ou de l'authenticité d'un message,

15 * dispositif de signature dans les cas de la preuve de l'origine et de l'intégrité d'un message,

III. Une troisième entité, appelée dispositif contrôleur, se présente notamment sous la forme d'un terminal et/ou d'un serveur distant connecté à un réseau de communication informatique. Le dispositif contrôleur vérifie l'authentification ou l'origine et l'intégrité d'un message,

20 L'objet nomade comporte des moyens de connexion pour connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique ledit dispositif témoin et/ou ledit dispositif pilote audit dispositif contrôleur.

25 Le dispositif témoin reçoit du dispositif pilote ou du dispositif contrôleur un ou plusieurs défis d tel que $0 \leq d \leq v_x - 1$ et comporte des deuxièmes moyens de calcul pour calculer à partir dudit défi d une ou plusieurs réponses D en effectuant des opérations du type :

$$D_i \equiv r_i \cdot Q A_i^d \bmod p_i$$

ou r_i est un aléa tel que $0 < r_i < p_i$.

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer par lesdits deuxièmes moyens de calcul pour calculer chacune des réponses D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

- 5 L'objet nomade comporte des moyens de transmission pour transmettre audit dispositif contrôleur la ou les dites réponses D .

Cas où l'exposant de vérification v est unique

De même que précédemment, l'objet nomade fait intervenir trois entités :

- 10 I. Une première entité, appelée dispositif témoin, est contenue dans ledit objet nomade. Le dispositif témoin dispose d'une première zone mémoire contenant des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$. Le dispositif témoin dispose aussi d'une deuxième zone mémoire contenant

- 15 * des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$,
..., représentant des clés privées QA, QB, \dots

- * des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

- * un exposant public de vérification v .

Les paires de clés privées et publiques sont liées par des relations du type :

20
$$GA \cdot QA' \bmod n \equiv 1 \text{ ou } GA \equiv QA' \bmod n$$

Le dispositif témoin comporte aussi des premiers moyens de calcul pour calculer des engagements R ,

- en effectuant des opérations du type :

$$R_i \equiv r_i^v \bmod p_i$$

- 25 où r_i est un entier, tiré au hasard, associé au nombre premier p_i , tel que $0 < r_i < p_i$, appartenant à au moins une collection d'aléas $\{r_1, r_2, r_3, \dots\}$,

- puis en appliquant la méthode des restes chinois,

Il y a autant d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$,

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer par

lesdits premiers moyens de calcul pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

II. Une deuxième entité est appelée dispositif pilote dudit dispositif témoin. Elle peut être également contenue dans ledit objet nomade. Le dispositif pilote est appelé :

* dispositif démonstrateur dans le cas de la preuve de l'authenticité d'une entité ou de l'authenticité d'un message,

* dispositif de signature dans les cas de la preuve de l'origine et de l'intégrité d'un message.

III. Une troisième entité, appelée dispositif contrôleur, se présente notamment sous la forme d'un terminal et/ou d'un serveur distant connecté à un réseau de communication informatique. Le dispositif contrôleur vérifie l'authentification ou l'origine et l'intégrité d'un message.

L'objet nomade comporte des moyens de connexion pour connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique ledit dispositif témoin et/ou ledit dispositif pilote audit dispositif contrôleur.

Le dispositif témoin reçoit du dispositif pilote ou du dispositif contrôleur, des collections de défis d $\{dA, dB, \dots\}$ tels que $0 \leq dA \leq v - 1$. Le nombre des collections de défis d étant égal au nombre d'engagements R . Chaque collection $\{dA, dB, \dots\}$ comprend un nombre de défis égal au nombre de paires de clés.

Le dispositif témoin comporte des deuxièmes moyens de calcul pour calculer à partir de chacune desdites collections de défis $\{dA, dB, \dots\}$ des réponses D . A cet effet,

- il effectue des opérations du type :

$$D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \bmod p_i$$

- puis, il appliquant la méthode des restes chinois.

Il y a autant de réponses **D** que d'engagements **R** et de défis **d**.

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer par lesdits deuxièmes moyens de calcul pour calculer chacun des D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo **n**.

L'objet nomade comporte des moyens de transmission pour transmettre audit dispositif contrôleur la ou lesdites réponses **D**.

On va maintenant exposer des variantes de réalisation de l'objet nomade selon l'invention concernant :

- le cas d'une authentification d'entité,
- le cas d'une authentification de message,
- le cas d'une signature numérique de message.

Cas d'une authentification d'entité

Cas où l'exposant de vérification v est unique.

Dans le cas de cette variante de réalisation particulière, la session est destinée à prouver à un dispositif contrôleur l'authenticité d'une entité.

Comme dans le cas général, la session fait intervenir trois entités.

I. Une première entité, appelée dispositif témoin, est contenue dans ledit objet nomade. Le dispositif témoin comporte une première zone mémoire contenant des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public **n** tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$. Le dispositif témoin comporte aussi une deuxième zone mémoire contenant :

* des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ..., représentant des clés privées **QA**, **QB**, ...

* des clés publiques **GA**, **GB**, ... ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

* un exposant public de vérification **v**.

Les paires de clés privées et publiques sont liées par des relations du type :

$$GA \cdot QA' \bmod n \equiv 1 \text{ ou } GA \equiv QA' \bmod n$$

II. Une deuxième entité est appelée dispositif démonstrateur du dispositif témoin. Elle peut être également contenue dans ledit objet nomade.

III. Une troisième entité, appelée dispositif contrôleur, se présente notamment sous la forme d'un terminal et/ou d'un serveur distant connecté à un réseau de communication informatique.

L'objet nomade comporte des moyens de connexion pour connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique ledit dispositif témoin et/ou ledit dispositif démonstrateur audit dispositif contrôleur.

Pour prouver l'authenticité d'une entité, ledit objet nomade exécute les étapes suivantes :

• **étape 1. engagement R du dispositif témoin :**

Le dispositif témoin comporte des premiers moyens de calcul pour tirer au hasard et en privé, à chaque appel, au moins une collection de nombres entiers $\{r_1, r_2, r_3, \dots\}$, telle que, pour chaque facteur premier p_i , chaque collection comporte un aléa r_i positif et plus petit que p_i .

Le dispositif témoin comporte des deuxièmes moyens de calcul pour élever chaque aléa r_i à la puissance v ième modulo p_i , pour chaque facteur premier p_i ,

$$R_i \equiv r_i^v \text{ mod } p_i$$

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer par les deuxièmes moyens de calcul pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n)

Puis, lesdits deuxièmes moyens de calcul du dispositif témoin établissent chaque engagement R modulo n selon la méthode des restes chinois.

Il y a autant d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$.

• **étape 2. transmission des engagements R et réception des défis d destinés au dispositif témoin :**

5

10

15

20

25

I. Une première entité, appelée dispositif témoin, est contenue dans ledit

objet nomade,.

Le dispositif témoin comporte une première zone mémoire contenant des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$. Le dispositif témoin comporte aussi une deuxième zone mémoire contenant

* des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ..., représentant des clés privées QA, QB, \dots

* des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

* un exposant public de vérification v .

Les paires de clés privées et publiques sont liées par des relations du type :

$$GA \cdot QA' \bmod n \equiv 1 \text{ ou } GA \equiv QA' \bmod n$$

II. Une deuxième entité, est appelée démonstrateur dudit dispositif témoin. Elle peut être également contenue dans ledit objet nomade.

III. Une troisième entité appelée dispositif contrôleur se présente sous la forme d'un terminal et/ou d'un serveur distant connecté à un réseau de communication informatique.

L'objet nomade comporte des moyens de connexion pour connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique ledit dispositif témoin et/ou ledit dispositif démonstrateur audit dispositif contrôleur.

Pour prouver l'authenticité d'un message ledit objet nomade exécute les étapes suivantes :

• **étape 1. engagement R du dispositif témoin :**

Le dispositif témoin comporte des premiers moyens de calcul pour tirer au hasard et en privé, à chaque appel, au moins une collection de nombres entiers $\{r_1, r_2, r_3, \dots\}$, telle que, pour chaque facteur premier p_i , chaque collection comporte un aléa r_i positif et plus petit que p_i .

Le dispositif témoin comporte des deuxièmes moyens de calcul pour élever

chaque aléa r_i à la puissance v ième modulo p_i , pour chaque facteur premier p_i ,

$$R_i \equiv r_i^v \text{ mod } p_i$$

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer par les
5 deuxièmes moyens de calcul pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

Puis, lesdits deuxièmes moyens de calcul dudit dispositif témoin établissent chaque engagement R modulo n selon la méthode des restes chinois.

10 Il y a autant d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$.

• **étape 2. réception des défis d destinés au dispositif témoin:**

Le dispositif démonstrateur comporte des premiers moyens de calcul pour calculer un jeton T , en appliquant une fonction de hachage f ayant comme arguments le message m et chaque engagement R . L'objet nomade
15 comporte des moyens de transmission pour transmettre audit dispositif contrôleur le jeton T . L'objet nomade comporte des moyens de réception pour recevoir des collections de défis d $\{dA, dB, \dots\}$ produits par ledit dispositif contrôleur au moyen du jeton T .

• **étape 3. réponse du dispositif témoin au défi d :**

20 Le dispositif témoin comporte des troisièmes moyens de calcul pour calculer des réponses D , à partir desdites collections de défis d $\{dA, dB, \dots\}$ reçues du dispositif contrôleur. A cet effet, il effectuant des opérations du type :

$$D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \text{ mod } p_i$$

25 puis, il applique la méthode des restes chinois.

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer par les quatrièmes moyens de calcul pour calculer chacun des D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n

Il y a autant de réponses **D** calculées par le témoin que d'engagements **R** et de défis **d**.

• **étape 4. données destinées au dispositif contrôleur :**

L'objet nomade comporte des moyens de transmission pour transmettre
5 audit dispositif contrôleur chaque réponse **D**.

• **étape 5. vérification par le dispositif contrôleur :**

Le dispositif contrôleur vérifie la cohérence des triplets **{R, d, D}** et l'authenticité du message **m**.

Cas d'une signature numérique de message

Cas où l'exposant de vérification v est unique.

Dans le cas de cette variante de réalisation particulière, la session est destinée à prouver à un contrôleur la signature numérique d'un message **m**.

Comme dans le cas général, l'objet nomade fait intervenir trois entités :

I. Une première entité, appelée dispositif témoin, est contenue dans ledit
15 objet nomade. Le dispositif témoin comporte une première zone mémoire contenant des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public **n** tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$. Le dispositif témoin comporte aussi une deuxième zone mémoire contenant :

* des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$,
20 ..., représentant des clés privées **QA, QB, ...**

* des clés publiques **GA, GB, ...** ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

* un exposant public de vérification **v**.

Les paires de clés privées et publiques sont liées par des relations du type :

$$GA \cdot QA^v \bmod n \equiv 1 \text{ ou } GA \equiv QA^v \bmod n$$

II. Une deuxième entité est appelée dispositif de signature. Elle peut être également contenue dans ledit objet nomade.

III. Une troisième entité appelée dispositif contrôleur se présente sous la forme d'un terminal et/ou d'un serveur distant connecté à un réseau de

communication informatique.

L'objet nomade comporte des moyens de connexion pour connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique ledit dispositif témoin et ledit dispositif de signature audit dispositif contrôleur.

Pour prouver la signature d'un message ledit objet nomade exécute les étapes suivantes :

• **étape 1. engagement R du dispositif témoin :**

Le dispositif témoin comporte des premiers moyens de calcul pour tirer au hasard et en privé, à chaque appel, au moins une collection de nombres entiers $\{r_1, r_2, r_3, \dots\}$, telle que, pour chaque facteur premier p_i , chaque collection comporte un aléa r_i positif et plus petit que p_i .

Le dispositif témoin comporte des deuxièmes moyens de calcul pour élever chaque aléa r_i à la puissance v ième modulo p_i , pour chaque facteur premier p_i ,

$$R_i \equiv r_i^v \bmod p_i$$

Puis, lesdits deuxièmes moyens de calcul dudit dispositif témoin établissent chaque engagement R modulo n selon la méthode des restes chinois.

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer par les deuxièmes moyens de calcul pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

Il y a autant d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$.

• **étape 2. défi d destiné au dispositif témoin :**

Le dispositif de signature comporte des troisièmes moyens de calcul pour calculer, en appliquant une fonction de hachage f ayant comme arguments le message m et chaque engagement R , au moins une collection de défis d $\{dA, dB, \dots\}$ tels que $0 \leq dA \leq v - 1$. Le nombre des collections de défis d étant égal au nombre d'engagements R . Chaque collection $\{dA, dB, \dots\}$

comprend un nombre de défis égal au nombre de paires de clés.

Le dispositif de signature transmet les collections de défis **d** au dispositif témoin.

• **étape 3. réponse du dispositif témoin au défi d :**

5 Le dispositif témoin comporte des quatrièmes moyens de calcul pour calculer des réponses **D**, à partir desdites collections de défis **d** {**dA**, **dB**, ...} reçues du dispositif contrôleur. A cet effet, il effectue des opérations du type :

$$D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \text{ mod } p_i$$

10 puis, il appliquant la méthode des restes chinois.

Ainsi, le nombre d'opérations arithmétiques modulo **p_i** à effectuer par les quatrièmes moyens de calcul pour calculer chacun des **D_i** pour chacun des **p_i** est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo **n**.

15 Il y a autant de réponses **D** calculées par le témoin que d'engagements **R** et de défis **d**.

L'objet nomade comporte des moyens de transmission pour transmettre les réponses **D** au dispositif de signature et/ou au dispositif contrôleur.

• **étape 4. données destinées au dispositif contrôleur :**

20 L'objet nomade comporte des moyens de transmission pour transmettre au dispositif contrôleur un message signé comprenant :

- le message **m**,
- les collections de défis **d** ou les engagements **R**,
- chaque réponse **D**

25 • **étape 5. vérification par le dispositif contrôleur :**

Le dispositif contrôleur vérifie la cohérence des triplets {**R**, **d**, **D**} et la signature numérique du message **m**.

Paire de clés conférant une sécurité équivalente à la connaissance de la clé privée Q

La paire de clés GA, QA, \dots n'a plus de raison d'être systématiquement déduite de l'identité du témoin, comme dans le cas du procédé GQ.

Dans le cas de la variante ci-après exposée les composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ... des clés privées QA, QB, \dots sont des nombres tirés au hasard à raison d'une composante QA_i, QB_i, \dots pour chacun desdits facteurs premiers p_i , lesdites clés privées QA, QB , pouvant être calculées à partir desdites composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, par la méthode des restes chinois.

Le dispositif témoin comporte des huitièmes moyens de calcul pour calculer lesdites clés publiques GA, GB, \dots ,

- en effectuant des opérations du type :

$$GA_i \equiv QA_i' \pmod{p_i}$$

- puis en appliquant la méthode des restes chinois pour établir GA tel que

$$GA \equiv QA' \pmod{n}$$

ou bien tel que

$$GA \cdot QA' \pmod{n} \equiv 1$$

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer par les huitièmes moyens de calcul dudit dispositif témoin pour calculer chacun des GA_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

De préférence, l'exposant public de vérification v est un nombre premier. Il en résulte que la paire de clés GA, QA confère une sécurité équivalente à la connaissance de la clé privée QA .

Paire de clés conférant une sécurité équivalente à la connaissance de la factorisation de n

De préférence, l'exposant public de vérification v est du type

$$v = a^k$$

où k est un paramètre de sécurité plus grand que 1.

De préférence également, l'exposant public de vérification v est du type

$$v = 2^k$$

où k est un paramètre de sécurité plus grand que 1.

Dans ce cas, la clé publique GA est un carré gA^2 inférieur à n choisi de sorte que les deux équations

$$x^2 \equiv gA \pmod{n} \quad \text{et} \quad x^2 \equiv -gA \pmod{n}$$

n'ont pas de solution en x dans l'anneau des entiers modulo n .

Le dispositif témoin comportant des neuvièmes moyens de calcul pour calculer lesdites composantes $QA_1, QA_2, \dots (QA_i, \dots)$ de la clé privée QA en appliquant des formules telles que :

$$GA \equiv QA_i^{2 \cdot \exp(k)} \pmod{p_i}$$

ou bien telles que :

$$GA \cdot QA_i^{2 \cdot \exp(k)} \pmod{p_i} \equiv 1$$

et en extrayant la k ième racine carrée de GA dans le corps de Galois $CG(p_i)$.

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer par les neuvièmes moyens de calcul du dispositif témoin pour calculer chacun des QA_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

On démontre que la paire de clés GA, QA confère une sécurité équivalente à la connaissance de la factorisation de n .

De préférence, pour extraire la k ième racine carrée de GA dans le corps de Galois $CG(p_i)$, on utilise les méthodes suivantes :

* dans le cas où le facteur premier p_i est congru à 3 modulo 4, les neuvièmes moyens de calcul du dispositif témoin appliquent notamment un algorithme du type :

$$x = (p+1)/4 ; y \equiv x^k \pmod{p-1} ; z = y ; QA_i \equiv GA^z \pmod{p_i}$$

* dans le cas où le facteur premier p_i est congru à 1 modulo 4, les neuvièmes moyens de calcul du dispositif témoin appliquent notamment un algorithme basé sur les suites de Lucas.

Terminal ou Serveur distant

Concept général GQ2

La présente invention concerne également un dispositif de contrôle, se présentant sous la forme d'un terminal ou d'un serveur distant connecté à un réseau de communication informatique.

Le terminal ou le serveur selon l'invention permet de mettre en œuvre le procédé ci-dessus exposé et de diminuer la charge de travail pendant une session destinée à vérifier :

- l'authenticité d'une entité et/ou
- l'origine et l'intégrité d'un message m .

Le dispositif de contrôle met en œuvre :

- un module public n tel que n soit le produit de facteurs premiers secrets $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2)

$$n = p_1 \cdot p_2 \cdot p_3 \cdot \dots ,$$

- des clés publiques GA, GB, \dots
- des exposants publics de vérification vx, vy, \dots

lesdites clés privées GA et les clés publiques associées QA étant liées par des relations du type :

$$GA \cdot QA^{vx} \bmod n \equiv 1 \text{ ou } GA \equiv QA^{vy} \bmod n$$

Le dispositif de contrôle fait intervenir trois entités.

I. Une première entité, appelée dispositif témoin, contenue notamment dans un objet nomade se présentant par exemple sous la forme d'une carte bancaire à microprocesseur. Le dispositif témoin produit des engagements R et des réponses D à des défis d .

II. Une deuxième entité est appelée dispositif pilote dudit dispositif témoin. Elle peut être contenue notamment dans ledit objet nomade.

III. Une troisième entité, appelée dispositif contrôleur, est contenue dans ledit dispositif de contrôle.

Le dispositif de contrôle comporte :

- des moyens de connexion pour connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique ledit dispositif contrôleur audit dispositif témoin et/ou audit dispositif pilote,

- des moyens de transmission pour transmettre les données produites par ledit dispositif contrôleur vers ledit dispositif témoin et/ou ledit dispositif pilote,

- des moyens de réception pour recevoir les données provenant dudit dispositif témoin et/ou dudit-dispositif pilote.

Le dispositif contrôleur comporte :

- des premiers moyens de calcul pour produire un ou plusieurs défis d tel que $0 \leq d \leq v_x - 1$,

- des deuxièmes moyens de calcul pour calculer, en fonction des réponses D reçues dudit dispositif témoin et/ou dudit dispositif pilote, des engagements R' en effectuant des opérations du type :

$$R'_i \equiv GA^d \cdot D^{v_x} \bmod n$$

ou du type :

$$R'_i \cdot GA^d \equiv D^{v_x} \bmod n$$

- des troisièmes moyens de calcul pour vérifier que les triplets $\{R', d, D\}$ sont cohérents.

Cas où l'exposant de vérification v est unique

De même que précédemment, ledit dispositif de contrôle se présente sous la forme d'un terminal ou d'un serveur distant connecté à un réseau de communication informatique. Il met en œuvre :

- un module public n tel que n soit le produit de facteurs premiers secrets $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2)

$$n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$$

- des clés publiques GA, GB, \dots

- un exposant public de vérification v

Les clés privées GA et les clés publiques associées QA sont liées par des

relations du type :

$$GA.QA' \bmod n \equiv 1 \text{ ou } GA \equiv QA' \bmod n$$

ledit dispositif de contrôle fait intervenir trois entités :

I. Une première entité, appelée dispositif témoin, est contenue notamment dans un objet nomade se présentant par exemple sous la forme d'une carte bancaire à microprocesseur. Le dispositif témoin produit des engagements **R** et des réponses **D** à des défis **d**.

II. Une deuxième entité est appelée dispositif pilote dudit dispositif témoin. Elle peut être contenue notamment dans ledit objet nomade.

III. Une troisième entité, appelée dispositif contrôleur, est contenue dans ledit dispositif de contrôle.

Le dispositif de contrôle comporte :

- des moyens de connexion pour connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique ledit dispositif contrôleur audit dispositif témoin et/ou audit dispositif pilote,

- des moyens de transmission pour transmettre les données produites par ledit dispositif contrôleur vers ledit dispositif témoin et/ou ledit dispositif pilote,

- des moyens de réception pour recevoir les données provenant dudit dispositif témoin et/ou dudit dispositif pilote,

Le dispositif contrôleur comporte :

- des premiers moyens de calcul pour produire un ou plusieurs défis **d** {**dA**, **dB**, ...} tels que $0 \leq dA \leq v - 1$,

- des deuxièmes moyens de calcul pour calculer, en fonction des réponses **D** reçues du dudit dispositif témoin et/ou dudit dispositif pilote, des engagements **R'**, en effectuant des opérations du type :

$$R' \equiv GA^{dA} \cdot GB^{dB} \cdot \dots D' \bmod n$$

ou du type :

$$R' \cdot GA^{dA} \cdot GB^{dB} \cdot \dots \equiv D' \bmod n$$

- des troisièmes moyens de calcul pour vérifier que les triplets $\{R', d, D\}$ sont cohérents.

Cas d'une authentification d'entité

Cas où l'exposant de vérification v est unique.

5 Dans le cas de cette variante de réalisation, la session est destinée à vérifier l'authenticité d'une entité. Dans le cas d'une authentification d'entité, le dispositif pilote est appelé dispositif démonstrateur.

Pour prouver l'authenticité d'une entité ledit dispositif de contrôle exécute les étapes suivantes :

10 • étape 1. engagement R du dispositif témoin :

Le dispositif témoin produit au moins un engagement R à partir d'au moins une collection d'aléas $\{r_1, r_2, r_3, \dots\}$, telle que, pour chaque facteur premier p_i , chaque collection comporte un aléa r_i entier positif et plus petit que p_i . Il y a autant d'engagements R que de collections d'aléas.

15 • étape 2. défis produits par le dispositif contrôleur et destinés au dispositif témoin :

Les moyens de réception du dispositif de contrôle reçoivent tout ou partie de chaque engagement R , transmis par le dispositif démonstrateur, et le transmettent au dispositif contrôleur.

20 Le dispositif contrôleur comporte des premiers moyens de calcul pour calculer, après avoir reçu tout ou partie de chaque engagement R , au moins une collection de défis d $\{dA, dB, \dots\}$ tels que $0 \leq dA \leq v - 1$. Le nombre des collections de défis d est égal au nombre d'engagements R . Chaque collection $\{dA, dB, \dots\}$ comprend un nombre de défis égal au nombre de paires de clés.

25 • étape 3. réponse du dispositif témoin aux défis d :

Le dispositif témoin comporte des quatrièmes moyens de calcul pour calculer des réponses D , à partir desdites collections de défis d $\{dA, dB, \dots\}$ reçues du dispositif contrôleur. Il y a autant de réponses D que

d'engagements R et de défis d .

• **étape 4. données destinées au dispositif contrôleur :**

Les moyens de réception du dispositif de contrôle reçoivent du dispositif démonstrateur chaque réponse D .

5

• **étape 5. vérification par le dispositif contrôleur :**

Le dispositif contrôleur comporte des deuxièmes moyens de calcul pour calculer à partir de chaque réponse D un engagement R' en effectuant des opérations du type :

$$R' \equiv GA^{d_A} \cdot GB^{d_B} \cdot \dots D' \bmod n$$

10

ou du type :

$$R' \cdot GA^{d_A} \cdot GB^{d_B} \cdot \dots \equiv D' \bmod n$$

Le dispositif contrôleur comporte des troisièmes moyens de calcul pour comparer et vérifier que chaque engagement reconstruit R' reproduit tout ou partie de chaque engagement R transmis à l'étape 2 par le dispositif démonstrateur.

15

Cas d'une authentification de message

Cas où l'exposant de vérification v est unique.

Dans le cas de cette variante de réalisation particulière, la session est destinée à vérifier l'authenticité d'un message m . Dans le cas d'une authentification d'un message m , le dispositif pilote est appelé dispositif démonstrateur.

20

Pour prouver l'authenticité d'un message m , ledit dispositif de contrôle exécute les étapes suivantes :

• **étape 1. engagement R du dispositif témoin :**

25

Le dispositif témoin produit au moins un engagement R à partir d'au moins une collection d'aléas $\{r_1, r_2, r_3, \dots\}$, telle que, pour chaque facteur premier p_i , chaque collection comporte un aléa r_i entier positif et plus petit que p_i . Il y a autant d'engagements R que de collections d'aléas.

• **étape 2. défis d produits par ledit dispositif contrôleur et**

destinés au dispositif témoin :

Les moyens de réception du dispositif de contrôle reçoivent un jeton **T** calculé et transmis par le dispositif démonstrateur en appliquant une fonction de hachage **f** ayant comme arguments le message **m** et chaque engagement **R**.

Le dispositif contrôleur comporte des premiers moyens de calcul pour calculer, après avoir reçu le jeton **T**, au moins une collection de défis **d** {**dA**, **dB**, ...} tels que $0 \leq dA \leq v - 1$. Le nombre des collections de défis **d** est égal au nombre d'engagements **R**. Chaque collection {**dA**, **dB**, ...} comprend un nombre de défis égal au nombre de paires de clés.

• étape 3. réponse du dispositif témoin au défi d :

Le dispositif témoin comporte des quatrièmes moyens de calcul pour calculer des réponses **D**, à partir desdites collection de défis **d** {**dA**, **dB**, ...} reçues du dispositif contrôleur. Il y a autant de réponses **D** calculées par le témoin que d'engagements **R** et de défis **d**.

• étape 4. données destinées au dispositif contrôleur :

Les moyens de réception du dispositif de contrôle reçoivent du dispositif démonstrateur chaque réponse **D**.

• étape 5. vérification par le dispositif contrôleur :

Le dispositif contrôleur comporte des deuxièmes moyens de calcul pour calculer à partir de chaque réponse **D** un engagement **R'** en effectuant des opérations du type :

$$R' \equiv GA^{dA} \cdot GB^{dB} \cdot \dots D^v \mod n$$

ou du type :

$$R' \cdot GA^{dA} \cdot GB^{dB} \cdot \dots \equiv D^v \mod n$$

Le dispositif contrôleur comporte des troisièmes moyens de calcul pour calculer un jeton **T'**, en appliquant la fonction de hachage **f** ayant comme arguments le message **m** et chaque engagement **R'**.

Le dispositif contrôleur comporte des quatrièmes moyens de calcul pour

comparer et vérifier que le jeton T' est identique au jeton T transmis à l'étape 2 par le dispositif démonstrateur.

Cas d'une signature numérique de message

Cas où l'exposant de vérification v est unique

5 Dans le cas de cette variante de réalisation particulière, la session est destinée à vérifier la signature numérique d'un message m . Dans le cas d'une authentification d'un message m , le dispositif pilote est appelé dispositif de signature.

10 Pour prouver la signature numérique du message m , ledit dispositif de contrôle exécute les étapes suivantes :

• étape 1. engagement R du témoin :

Le dispositif témoin produit au moins un engagement R à partir d'au moins une collection d'aléas $\{r_1, r_2, r_3, \dots\}$, telle que, pour chaque facteur premier p_i , chaque collection comporte un aléa r_i entier positif et plus petit que p_i .
15 Il y a autant d'engagements R que de collections d'aléas.

• étape 2. défis d destinés au dispositif témoin :

Le dispositif de signature calcule, en appliquant une fonction de hachage f ayant comme arguments le message m et chaque engagement R , au moins une collection de défis d $\{dA, dB, \dots\}$ tels que $0 \leq dA \leq v - 1$. Le nombre
20 des collections de défis d est égal au nombre d'engagements R . Chaque collection $\{dA, dB, \dots\}$ comprend un nombre de défis égal au nombre de paires de clés.

Le dispositif de signature transmet les collections de défis d au dispositif témoin.

25 • étape 3. réponse du dispositif témoin au défi d :

Le dispositif témoin comporte des quatrièmes moyens de calcul pour calculer des réponses D , à partir desdites collections de défis d $\{dA, dB, \dots\}$. Il y a autant de réponses D calculées par le témoin que d'engagements R et de défis d .

Le dispositif témoin comporte des moyens de transmission pour transmettre les réponses **D** au dispositif de signature et/ou au dispositif contrôleur.

• **étape 4. données destinées au dispositif contrôleur :**

Les moyens de réception du dispositif de contrôle reçoivent du dispositif de signature un message signé comprenant :

- le message **m**,
- les collections de défis **d** ou les engagements **R**,
- chaque réponse **D**.

• **étape 5. vérification par le dispositif contrôleur :**

Cas où le dispositif contrôleur reçoit la collection des défis **d**

Dans ce cas, le dispositif contrôleur reçoit les collections des défis **d** et des réponses **D**.

Le dispositif contrôleur comporte :

- * des premiers moyens de calcul pour calculer à partir de chaque réponse **D** un engagement **R'** en effectuant des opérations du type :

$$R' \equiv GA^{d_A} \cdot GB^{d_B} \cdot \dots D^v \text{ mod } n$$

ou du type :

$$R' \cdot GA^{d_A} \cdot GB^{d_B} \cdot \dots \equiv D^v \text{ mod } n$$

- * des deuxièmes moyens de calcul pour calculer chaque défi **d'**, en appliquant la fonction de hachage **f** ayant comme arguments le message **m** et chaque engagement reconstruit **R'**,

- * des troisièmes moyens de calcul pour comparer et vérifier que chaque défi **d'** est identique au défi **d** figurant dans le message signé.

Cas où le dispositif contrôleur reçoit la collection des engagements **R**

Dans ce cas, le dispositif contrôleur reçoit la collection des engagements **R** et des réponses **D**,

Le dispositif contrôleur comporte :

- * des premiers moyens de calcul pour calculer chaque défi **d'**, en appliquant la fonction de hachage **f** ayant comme arguments le message **m**

et chaque engagement R ,

* des deuxièmes moyens de calcul pour calculer, alors, la collection des engagements R' en effectuant des opération du type

$$R' \equiv GA^{d'A} \cdot GB^{d'B} \cdot \dots D' \bmod n$$

ou du type :

$$R' \cdot GA^{d'A} \cdot GB^{d'B} \cdot \dots \equiv D' \bmod n$$

* des troisièmes moyens de calcul pour comparer et vérifier que chaque engagement R' reconstruit est identique à l'engagement R figurant dans le message signé.

Paire de clés conférant une sécurité équivalente à la connaissance de la clé privée Q

La paire des clés GA, QA, \dots n'a plus raison d'être systématiquement déduite de l'identité du témoin, comme dans le cas du procédé GQ.

Dans le cas de la variante de réalisation ci-après exposée les composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, des clés privées QA, QB, \dots sont des nombres tirés au hasard à raison d'une composante QA_i, QB_i, \dots pour chacun desdits facteurs premiers p_i , lesdites clés privées QA, QB , pouvant être calculées à partir desdites composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ... par la méthode des restes chinois,

Le dispositif témoin comporte des moyens de calcul pour calculer les clés publiques GA, GB, \dots ,

• en effectuant des opérations du type :

$$GA_i \equiv QA_i' \bmod p_i$$

• puis, en appliquant la méthode des restes chinois pour établir GA tel que

$$GA \equiv QA' \bmod n$$

ou bien tel que

$$GA \cdot QA' \bmod n \equiv 1$$

Le nombre d'opérations arithmétiques modulo p_i à effectuer par les huitièmes moyens de calcul dudit dispositif témoin pour calculer chacun

des GA_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

De préférence, l'exposant public de vérification v est un nombre premier.

On peut démontrer que la paire de clés GA, QA confère une sécurité équivalente à la connaissance de la clé privée QA .

Paire de clés conférant une sécurité équivalente à la connaissance de la factorisation de n

De préférence, l'exposant public de vérification v est du type

$$v = a^k$$

où k est un paramètre de sécurité plus grand que 1.

De préférence également, l'exposant public de vérification v est du type

$$v = 2^k$$

où k est un paramètre de sécurité plus grand que 1,

Dans ce cas clé publique GA est un carré gA^2 inférieur à n choisi de sorte que les deux équations

$$x^2 \equiv gA \pmod{n} \quad \text{et} \quad x^2 \equiv -gA \pmod{n}$$

n'ont pas de solution en x dans l'anneau des entiers modulo n .

Le dispositif témoin comporte des neuvièmes moyens de calcul pour calculer les dites composantes $QA_1, QA_2, \dots (QA_i, \dots)$ de la clé privée QA en appliquant des formules telles que :

$$GA \equiv QA_i^{2 \exp(k)} \pmod{p_i}$$

ou bien telles que :

$$GA \cdot QA_i^{2 \cdot \exp(k)} \pmod{p_i} \equiv 1$$

et en extrayant la k ième racine carrée de GA dans le corps de Galois $CG(p_i)$.

Ainsi, le nombre d'opérations arithmétiques modulo p_i à effectuer par les neuvièmes moyens de calcul du dispositif témoin pour calculer chacun des QA_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

On peut démontrer que la paire de clés GA, QA confère une sécurité équivalente à la connaissance de la factorisation de n.

De préférence, pour extraire la k ième racine carrée de GA dans le corps de Galois $CG(p_i)$,

- 5 * dans le cas où le facteur premier p_i est congru à 3 modulo 4, les neuvièmes moyens de calcul du dispositif témoin appliquent notamment un algorithme du type :

$$x = (p+1)/4 ; y \equiv x^k \pmod{p-1} ; z = y ; QA_i \equiv GA^z \pmod{p_i}$$

- 10 * dans le cas où le facteur premier p_i est congru à 1 modulo 4, les neuvièmes moyens de calcul du dispositif témoin appliquent notamment un algorithme basé sur les suites de Lucas.

On va maintenant décrire de manière détaillée la présente invention en présentant dans une première partie les éléments mathématiques utilisés, puis, en développant dans une deuxième partie le procédé selon l'invention
15 appelé nouveau procédé.

Première partie : éléments mathématiques

1. Congruences

Dans ce paragraphe, x, y et z sont des entiers naturels. z n'est pas nul.

La notation « $x \equiv y \pmod{z}$ » se lit « x est congru à y (mod z) » ; elle est
20 équivalente à « z divise x-y ».

1.1. Propriétés de base des congruences

Les quatre lois suivantes sont utiles.

(Loi A)

$$\begin{aligned} & \{ a \equiv b \pmod{m}; x \equiv y \pmod{m} \} \\ 25 \quad & \Rightarrow \{ a \pm x \equiv b \pm y \pmod{m}; a.x \equiv b.y \pmod{m} \} \end{aligned}$$

(Loi B)

$$\begin{aligned} & \{ a.x \equiv b.y \pmod{m}; a \equiv b \pmod{m}; \text{pgcd}(a, m) = 1 \} \\ & \Rightarrow \{ x \equiv y \pmod{m} \} \end{aligned}$$

(Loi C)

$$\{ a \equiv b \pmod{m} \} \Leftrightarrow \{ a.n \equiv b.n \pmod{m.n} \}$$

(Loi D)

$$\{ a \equiv b \pmod{r.s}; \text{pgcd}(r,s)=1 \} \Leftrightarrow \{ a \equiv b \pmod{r}; a \equiv b \pmod{s} \}$$

5

1.2. Théorème de Fermat

Lorsque p est un nombre premier, $a^p \equiv a \pmod{p}$.

Démonstration.

La relation est triviale lorsque a est un multiple de p .

Définissons la suite $\{X\}$ pour un nombre entier a quelconque appartenant à $\{1, 2, 3, \dots, p-1\}$.

10

$$\{X\} = \{x_1 = a. \text{ Puis, pour } i \geq 1, x_{i+1} \equiv a + x_i \pmod{p}\}$$

Calculons le terme pour l'indice $i+p$:

$$x_{i+p} = x_i + p.a \equiv x_i \pmod{p}$$

Par conséquent, la suite $\{X\}$ est périodique et sa période est p .

15

Les $p-1$ premiers termes sont distincts et non nuls ; on y retrouve une fois et une seule fois chacun des entiers de 1 à $p-1$; les $p-1$ premiers termes forment donc une permutation des entiers de 1 à $p-1$.

Calculons le produit des $p-1$ premiers termes de la suite $\{X\}$.

Selon la loi A, $a.2a.3a. \dots (p-1)a \equiv 1.2.3. \dots (p-1) \pmod{p}$

20

Selon la loi B, $a^{p-1} \equiv 1 \pmod{p}$

Selon la loi A, $a^p \equiv a \pmod{p}$

1.3. Théorème d'Euler

La fonction d'Euler est notée par $\varphi(n)$. C'est le nombre d'entiers positifs inférieurs à n et premiers avec n .

25

\Rightarrow Lorsque a et n sont premiers entre eux,

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

\Rightarrow Lorsque n est un nombre premier p ,

$$\varphi(p) = p-1.$$

\Rightarrow Lorsque n est le produit de deux nombres premiers distincts p_1 et p_2 .

$$\varphi(n) = (p_1-1) \cdot (p_2-1).$$

\Rightarrow Lorsque la factorisation de n est $p_1^x \cdot p_2^y \cdot p_3^z \dots$,

$$\varphi(n)/n = (1-1/p_1) \cdot (1-1/p_2) \cdot (1-1/p_3) \dots$$

1.4. Rang des éléments dans le corps de Galois $\text{CG}(p)$

5 Soit un nombre premier impair p . Soit un nombre entier positif a inférieur à p . Définissons la suite $\{X\}$.

$$\{X\} = \{x_1 = a. \text{ Puis, pour } i \geq 1, x_{i+1} \equiv a \cdot x_i \pmod{p}\}$$

Calculons le terme pour l'indice $i+p$ et utilisons le théorème de Fermat.

$$x_{i+p} = a^p \cdot x_i \equiv a \cdot x_i \equiv x_{i+1} \pmod{p}$$

10 Par conséquent, la période de la suite $\{X\}$ est égale à $p-1$ ou à un diviseur de $p-1$. Cette période dépend de la valeur de a . Par définition, cette période est appelée « le rang de $a \pmod{p}$ ».

$$x_{\text{rang}(a, p)} \equiv 1 \pmod{p}$$

15 Les éléments de $\text{CG}(p)$ ayant pour rang $p-1$ sont appelés les « éléments générateurs de $\text{CG}(p)$. » La dénomination est due au fait que leurs puissances successives dans $\text{CG}(p)$, c'est-à-dire, les termes de la suite $\{X\}$ pour les indices de 1 à $p-1$, forment une permutation de tous les éléments non nuls de $\text{CG}(p)$.

20 Soit un élément générateur a de $\text{CG}(p)$. Evaluons le rang de l'élément $a^i \pmod{p}$: ce rang s'exprime simplement en fonction de i et de $p-1$.

\Rightarrow Lorsque i est premier avec $p-1$, c'est $p-1$.

\Rightarrow Lorsque i divise $p-1$, c'est $(p-1)/i$.

\Rightarrow Dans tous les cas, c'est $(p-1)/\text{pgcd}(p-1, i)$.

25 Par conséquent, dans le corps $\text{CG}(p)$, il y a $\varphi(p-1)$ éléments générateurs où φ est la fonction d'Euler.

Par conséquent, dans le corps de Galois $\text{CG}(p)$ où $(p-1)/2$ est un nombre premier impair noté par p' ,

\Rightarrow il y a un seul élément de rang 1 : c'est 1,

\Rightarrow il y a un seul élément de rang 2 : c'est -1 ,

\Rightarrow il y a $p'-1$ éléments de rang p' ,

\Rightarrow il y a $p'-1$ éléments de rang $2.p'$; ce sont les éléments générateurs.

1.5. Fonction de Carmichael

La fonction de Carmichael de n est notée par $\lambda(n)$. C'est la valeur maximale du rang (mod n).

\Rightarrow Lorsque n est le produit de deux nombres premiers impairs p_1 et p_2 ,

$$\lambda(n) = \text{ppcm}(p_1-1, p_2-1).$$

\Rightarrow Lorsque a et b sont premiers entre eux,

$$\lambda(a.b) = \text{ppcm}(\lambda(a), \lambda(b)).$$

\Rightarrow Pour les puissances d'un nombre premier impair p ,

$$\lambda(p^e) = p^{e-1}.$$

\Rightarrow Pour les puissances de 2,

$$\lambda(2) = 1; \lambda(4) = 2; \lambda(2^e) = 2^{e-2}.$$

\Rightarrow Dans tous les cas, $\lambda(n)$ divise $\varphi(n)$. L'égalité n'intervient que lorsque n est premier.

1.6. Résidus quadratiques

Considérons l'équation $x^2 \equiv c \pmod{n}$ où l'entier positif c est inférieur à n et premier avec n .

- Lorsque l'équation a des solutions en x , on dit que c est un résidu quadratique (mod n).
- Lorsque l'équation n'a pas de solution en x , on dit que c est un résidu non quadratique (mod n).

L'ensemble des résidus quadratiques (mod n) forme un groupe (mod n) pour la multiplication. En effet, le produit de deux résidus quadratiques (mod n) est un résidu quadratique (mod n). En outre, le produit d'un résidu quadratique (mod n) par un résidu non quadratique (mod n) est un résidu non quadratique (mod n).

1.7. Structure du corps de Galois $\text{CG}(p)$

Pour tout nombre premier impair p , il y a $(p-1)/2$ résidus quadratiques (mod

p) et $(p-1)/2$ résidus non quadratiques (mod p). De plus, $1^2, 2^2, \dots, ((p-1)/2)^2$ forment un ensemble complet de résidus quadratiques (mod p).

Pour tout nombre premier impair p , chaque résidu quadratique (mod p) a exactement deux racines carrées dans $CG(p)$. En effet, pour tout un élément générateur a de $CG(p)$, a^i (mod p) est un résidu quadratique si et seulement si i est pair ; ses racines carrées sont alors $\pm a^{i/2}$ (mod p). Les éléments x et $p-x$ ont le même carré dans $CG(p)$.

Pour tout nombre premier p congru à 3 (mod 4), pour tout nombre x positif et plus petit que p , l'un des deux nombres x ou $p-x$ est un résidu quadratique (mod p) et l'autre un résidu non quadratique (mod p). Alors, la transformation « élever au carré (mod p) » permute l'ensemble des résidus quadratiques (mod p). L'ensemble des résidus quadratiques (mod p) est souvent noté par Q_p . Dans l'ensemble Q_p , les deux transformations « élever au carré (mod p) » et « prendre la racine carrée (mod p) » sont définies et inverses l'une de l'autre.

Remarque. Dans $CG(p)$, lorsque $(p-1)/2$ est un nombre premier impair p' , les résidus quadratiques (mod p) sont les $p'-1$ éléments de rang p' complétés par l'élément de rang 1, c'est-à-dire, 1.

Lorsque p est un nombre premier congru à 1 (mod 4), la propriété précédente peut se généraliser comme suit : si $p-1 = z \cdot 2^e$ où z est impair et e plus grand que 1, alors la transformation « élever au carré (mod p) » permute l'ensemble des nombres c de rang impair, c'est-à-dire, dont le rang divise z (c'est z lui-même ou bien un diviseur de z), c'est-à-dire, l'ensemble des nombres c tels qu'il y a des solutions en x à l'équation suivante :

$$x^{2^e} \equiv c \pmod{p}$$

D'une manière plus générale, dans l'ensemble des éléments de rang impair de $CG(p)$, l'opération « élever au carré (mod p) » est une permutation. La permutation inverse peut légitimement s'appeler « prendre la racine carrée (mod p). »

1.7.1. Fonction exponentielle sur $CG(p)$

Lorsque p est un nombre premier impair et que a est un élément générateur de $CG(p)$, la transformation « élever a à la puissance x ième (mod p) » permute les éléments non nuls de $CG(p)$. La permutation inverse est définie par « prendre le logarithme discret de y en base a dans $CG(p)$ ».

Lorsque a est un élément générateur de $CG(p)$,

$$x \mapsto y \equiv a^x \pmod{p} \Leftrightarrow y \mapsto x \equiv \log_a(y) \text{ dans } CG(p)$$

1.7.2. Fonction puissance sur $CG(p)$

Lorsque p est un nombre premier impair et que v est premier avec $p-1$, la transformation « élever x à la puissance v ième (mod p) » respecte le rang des éléments. Elle permute les éléments de $CG(p)$. La permutation inverse est définie par une autre transformation « élever y à une puissance s ième (mod p) » où $p-1$ divise $v.s-1$. On dit que l'exposant s est « inverse de l'exposant v (mod $p-1$) ». »

$$x \mapsto y \equiv x^v \pmod{p} \Leftrightarrow y \mapsto x \equiv y^s \pmod{p}$$

1.8. Symboles de Legendre et de Jacobi

Lorsque p est un nombre premier, on peut classer les entiers positifs en deux catégories : les multiples de p et les nombres premiers avec p . En outre, les nombres premiers avec p se classent eux-mêmes en deux catégories : les résidus quadratiques (mod p) et les résidus non quadratiques (mod p).

Legendre a introduit un symbole spécial noté par $(c \mid p)$. Le **symbole de Legendre** de l'entier positif c par rapport au nombre premier p prend les valeurs $+1$, -1 et 0 .

- $(c \mid p) = 0$ lorsque c est un multiple de p .
- $(c \mid p) = +1$ lorsque c est un résidu quadratique (mod p).
- $(c \mid p) = -1$ lorsque c est un résidu non quadratique (mod p).

La formule suivante établie par Euler permet de calculer le symbole de Legendre (en assimilant tout naturellement les valeurs -1 et $p-1$) ; cette

formule est encore appelée le « critère d'Euler. »

$$(c \mid p) \equiv c^{(p-1)/2} \pmod{p}$$

Le **symbole de Jacobi** généralise le symbole de Legendre. Les deux symboles sont notés de la même manière. Connaissant la factorisation de l'entier impair n , la formule suivante définit le symbole de Jacobi par rapport à n à partir du symbole de Legendre par rapport à chaque facteur premier de n .

$$\text{Si } n = p_1^{\alpha} p_2^{\beta} \dots, \text{ alors } (c \mid n) = (c \mid p_1)^{\alpha} (c \mid p_2)^{\beta} \dots$$

En d'autres termes, si a et b sont des entiers positifs impairs premiers avec c et c' ,

$$(c \mid a \cdot b) = (c \mid a) \cdot (c \mid b) \quad \text{et} \quad (c \mid a) \cdot (c' \mid a) = (c' \cdot c \mid a)$$

Attention, résidus quadratiques et éléments avec symbole de Jacobi égal à +1 ne coïncident pas.

* Tous les résidus quadratiques $(\text{mod } n)$ ont un symbole de Jacobi égal à +1.

* La valeur -1 du symbole de Jacobi caractérise exclusivement des résidus non quadratiques $(\text{mod } n)$.

* Lorsque n n'est pas premier, il y a des résidus non quadratiques dont le symbole de Jacobi vaut +1.

Voici la base de la loi de réciprocité quadratique, la « reine de la théorie des nombres » aux dires de Gauss. Lorsque m et n sont deux nombres premiers impairs distincts, deux cas se présentent :

- Ou bien, ils sont tous deux congrus à 3 $(\text{mod } 4)$; dans ce cas, une seule des deux équations suivantes, $x^2 \equiv m \pmod{n}$ et $x^2 \equiv n \pmod{m}$, a deux solutions en x .
- Ou bien, ils ne sont pas tous deux congrus à 3 $(\text{mod } 4)$; dans ce cas, les deux équations ont des solutions ou bien aucune des deux n'a de solution.

La loi de réciprocité quadratique lie les symboles de Jacobi $(m \mid n)$ et

$$u_i = \frac{\alpha^i - \beta^i}{\alpha - \beta} \quad \text{et} \quad v_i = \alpha^i + \beta^i$$

On vérifie alors simplement que les expressions sont encore vraies pour l'indice $i+2$. Or, elles sont vraies pour les indices 0 et 1. Par récurrence, elles sont donc vraies pour tout indice i positif ou nul.

5 Par la suite, on utilisera également les relations suivantes. Leur démonstration est triviale.

$$v_i^2 - \Delta u_i^2 = 4.P^i$$

Pour doubler l'indice,

$$u_{2.i} = u_i.v_i; \quad v_{2.i} = v_i^2 - 2.P^i$$

10 Pour retrancher un à l'indice,

$$u_{i-1} = (S.u_i - v_i)/2.P \quad \text{et} \quad v_{i-1} = (S.v_i - \Delta u_i)/2.P$$

Pour ajouter un à l'indice,

$$u_{i+1} = (S.u_i + v_i)/2 \quad \text{et} \quad v_{i+1} = (S.v_i + \Delta u_i)/2$$

Par ailleurs, les racines α et β s'expriment facilement en fonction de $S = \alpha + \beta$ et de $\sqrt{\Delta} = \alpha - \beta$.

15

$$\alpha = (S + \sqrt{\Delta})/2 \quad \text{et} \quad \beta = (S - \sqrt{\Delta})/2$$

Les expressions de u_i et v_i en fonction des racines α et β s'écrivent encore :

$$u_i = \left(\frac{S + \sqrt{\Delta}}{2\sqrt{\Delta}} \right)^i - \left(\frac{S - \sqrt{\Delta}}{2\sqrt{\Delta}} \right)^i \quad \text{et} \quad v_i = \left(\frac{S + \sqrt{\Delta}}{2} \right)^i + \left(\frac{S - \sqrt{\Delta}}{2} \right)^i$$

Développons les polynômes $(S + \sqrt{\Delta})^{2.k+1}$ et $(S - \sqrt{\Delta})^{2.k+1}$ et combinons leurs développements.

20

$$\begin{aligned} 2^{2.k}.u_{2.k+1} &= C_{2.k+1}^1 . S^{2.k} + C_{2.k+1}^3 . S^{2.k-2} . \Delta + \dots C_{2.k+1}^{2.k-1} . S^2 . \Delta^{k-1} + \Delta^k \\ &= \sum_{i=0}^k C_{2.k+1}^{2.i+1} . S^{2.(k-i)} . \Delta^i \\ 2^{2.k}.v_{2.k+1} &= S^{2.k+1} + C_{2.k+1}^2 . S^{2.k-1} . \Delta + \dots C_{2.k+1}^{2.k-2} . S^3 . \Delta^{k-1} + C_{2.k+1}^{2.k} . S . \Delta^k \\ &= \sum_{i=0}^k C_{2.k+1}^{2.i} . S^{2.(k-i)+1} . \Delta^i \end{aligned}$$

C'est ainsi que Lucas a découvert et établi le théorème suivant :

Lorsque p est un nombre premier impair ne divisant ni P , ni S , ni Δ , p divise $u_p - (\Delta \mid p)$ et $u_p - \Delta \mid p$.

2. Quelques méthodes pratiques de calcul

2.1. Racines carrées dans $CG(p)$

Lorsque $c^{(p-1)/2} \pmod{p}$ vaut $+1$, l'équation $x^2 \equiv c \pmod{p}$ a deux solutions dans le corps de Galois $CG(p)$; ces deux solutions sont appelées « racines carrées de $c \pmod{p}$ ».

2.1.1. Cas où p est congru à 3 (mod 4)

Selon le critère d'Euler, on a :

$$c^{(p-1)/2} \equiv 1 \pmod{p}, \text{ ce qui donne, } c^{(p+1)/2} \equiv c \pmod{p}.$$

Lorsque le nombre premier p est congru à 3 (mod 4), le nombre $(p+1)/4$ est un entier ; par conséquent, les deux racines carrées de c dans $CG(p)$ sont alors $\pm c^{(p+1)/4} \pmod{p}$.

2.1.2. Cas où p est congru à 1 (mod 4)

Lorsque p est congru à 1 (mod 4), on utilise les suites de Lucas pour calculer une racine carrée de $c \pmod{p}$. On affecte la valeur c au paramètre P . Puis, on cherche une valeur du paramètre S telle que le discriminant $\Delta = S^2 - 4.c$ soit un résidu non quadratique (mod p). On procède par essais successifs. En pratique, on part de $S = 1$, puis, on fait croître la valeur de S . Lorsque Δ est un résidu non quadratique par rapport à un nombre premier p impair ne divisant ni c , ni S , ni Δ , les suites de Lucas pour les indices $p+1$ et $p+2$ sur le corps $CG(p)$ sont dans l'état initial multiplié par c .

Or, on connaît les relations suivantes : $v_i^2 - \Delta.u_i^2 = 4.P^i$ et $u_{2,i} = u_i.v_i$

En d'autres termes, p divise alors u_{p+1} qui est égal au produit de $u_{(p+1)/2}$ par $v_{(p+1)/2}$. Par conséquent, p divise alors $u_{(p+1)/2}$ ou $v_{(p+1)/2}$. En fait, p ne peut diviser $v_{(p+1)/2}$; il divise donc $u_{(p+1)/2}$.

On obtient donc, $v_{(p+1)/2}^2 \equiv 4.c^{(p+1)/2} \pmod{p}$

Or, $c^{(p+1)/2} \equiv c \pmod{p}$

Par conséquent, le nombre : $x \equiv \frac{-1}{2} v_{(p+1)/2} \pmod{p}$ est alors une solution à l'équation : $x^2 \equiv c \pmod{p}$.

Les relations suivantes sont utilisées pour calculer les suites $\{U\}$ et $\{V\}$ ensemble.

5 Pour doubler l'indice, $u_{2,i} = u_i \cdot v_i$; $v_{2,i} = v_i^2 - 2 \cdot c^i$

Pour ajouter 1 à l'indice, $u_{i+1} = (S \cdot u_i + v_i)/2$; $v_{i+1} = (\Delta \cdot u_i + S \cdot v_i)/2$

La procédure suivante utilise trois variables : x pour u , y pour v , et z pour c^i . L'indice cible est $(p+1)/2$; il est codé par une séquence de j bits. Cette séquence est examinée du bit de poids fort au bit de poids faible.

10 1. Donner à x la valeur 0 ; donner à y la valeur 2 ; donner à z la valeur 1.

2. Répéter j fois la séquence suivante.

Remplacer x par $x \cdot y \pmod{p}$.

Remplacer y par $y^2 - 2 \cdot z \pmod{p}$

Remplacer z par $z^2 \pmod{p}$.

15 Si le j ième bit codant l'indice cible vaut 1, exécuter la séquence suivante.

Remplacer t par x .

Remplacer x par $(S \cdot t + y)/2 \pmod{p}$.

Remplacer y par $(S \cdot t + \Delta \cdot y)/2 \pmod{p}$

20 Remplacer z par $z \cdot c \pmod{p}$.

3. Remplacer y par $y/2 \pmod{p}$. Le résultat cherché est y .

2.2. Algorithme d'Euclide

L'algorithme d'Euclide opère la division des entiers. Soient deux entiers positifs x et y tels que x soit plus grand que y . Divisons x par y pour obtenir un quotient q positif et plus petit que ou égal à x et un reste r positif ou nul et plus petit que y .

Soit, $0 < y < x$

Par conséquent, $x = q \cdot y + r$ avec $0 < q \leq x$ et $0 \leq r < y$

2.2.1. Coefficients de Bezout et pgcd

Par définition, les coefficients de Bezout de deux entiers positifs x et y sont deux entiers k et l définis de manière unique par :

$$0 \leq k < y, \quad 0 \leq l < x \quad \text{et} \quad k.x - l.y = \pm \text{pgcd}(x, y)$$

Par divisions successives, l'algorithme d'Euclide permet de calculer efficacement les coefficients de Bezout et le plus grand commun diviseur de deux entiers positifs.

A partir des valeurs initiales $C_0 = x$ et $C_1 = y$, considérons les divisions successives :

$$C_0 = q_1.C_1 + C_2; \quad C_1 = q_2.C_2 + C_3; \quad \dots$$

$$\text{jusqu'à: } C_{L-1} = q_L.C_L + C_{L+1} \text{ où } C_{L+1} = 0.$$

Les restes successifs forment la suite $\{C\}$ qui est ainsi définie pour les indices i allant de 0 à $L+1$.

Les quotients successifs forment la suite $\{q\}$ qui est ainsi définie pour les indices i allant de 1 à L .

La suite $\{C\}$ peut encore se définir de la manière suivante.

$\{C\} = \{C_0 = x; C_1 = y; \text{ puis, pour } i \text{ allant de } 1 \text{ à } L, C_{i+1} \equiv C_{i-1} - q_i.C_i\}$
 \Rightarrow La suite $\{C\}$ est strictement décroissante de C_0 jusqu'à C_{L+1} qui est nul.

Définissons maintenant deux autres suites appelées $\{A\}$ et $\{B\}$.

$$\{A\} = \{A_0 = 1; A_1 = 0; \text{ puis, pour } i \text{ allant de } 1 \text{ à } L, A_{i+1} \equiv A_{i-1} + q_i.A_i\}$$

$$\{B\} = \{B_0 = 0; B_1 = 1; \text{ puis, pour } i \text{ allant de } 1 \text{ à } L, B_{i+1} \equiv B_{i-1} + q_i.B_i\}$$

Les premiers termes de la suite $\{A\}$ sont

$$A_0 = 1, A_1 = 0, A_2 = 1, A_3 = q_2, A_4 = 1 + q_2 \cdot q_3, \dots$$

\Rightarrow La suite $\{A\}$ est strictement croissante de A_3 à A_{L+1} .

Les premiers termes suivants de la suite $\{B\}$ sont

$$B_0 = 0, B_1 = 1, B_2 = q_1, B_3 = 1 + q_1 \cdot q_2, \dots$$

\Rightarrow La suite $\{B\}$ est strictement croissante de B_2 à B_{L+1} .

En éliminant q_i entre les définitions des suites $\{A\}$ et $\{C\}$, nous obtenons :

$$A_i.C_{i+1} + A_{i+1}.C_i = A_{i-1}.C_i + A_i.C_{i-1}$$

Par conséquent, la valeur de $A_i.C_{i+1} + A_{i+1}.C_i$ est constante pour i allant de

0 à L .

Puisque $A_0.C_1 + A_1.C_0 = y$, nous obtenons : $A_{L+1}.C_L = y$,

Et, de la même manière, $B_{L+1}.C_L = x$.

Par ailleurs, remarquons les égalités : $x.A_0 - y.B_0 = x = (-1)^0.C_0$

5

$$x.A_1 - y.B_1 = -y = (-1)^1.C_1$$

Supposons la relation vraie pour les indices $i-1$ et i ; puis, vérifions qu'elle est encore vraie pour l'indice $i+1$.

$$\begin{aligned} x.A_{i+1} - y.B_{i+1} &= x.(A_{i-1} + q_i.A_i) - y.(B_{i-1} + q_i.B_i) \\ &= (x.A_{i-1} - y.B_{i-1}) + q_i.(x.A_i - y.B_i) = (-1)^{i-1}.(C_{i-1} - q_i.C_i) = (-1)^{i+1}.C_{i+1} \end{aligned}$$

10

Par récurrence, pour i allant de 1 à L , $x.A_i - y.B_i = (-1)^i.C_i$

En particulier, on obtient finalement : $x.A_L - y.B_L = (-1)^L.C_L$

Les coefficients de Bezout de x et y sont égaux à A_L et B_L .

Le plus grand commun diviseur de x et y est égal à C_L .

Exemple. Calculer les coefficients de Bezout de 10 103 et 63 659.

k	A	B	C	q
0	1	0	63 659 = x	-
1	0	1	10 103 = y	6
2	1	6	3 041	3
3	3	19	980	3
4	10	63	101	9
5	93	586	71	1
6	103	649	30	2
7	299	1 884	11	2
8	701	4 417	8	1
9	1 000	6 301	3	2
10	2 701	17 019	2	1

$11 = L$	$3\ 701 = A_L$	$23\ 320 = B_L$	$1 = C_L$	2
12	$10\ 103 = y$	$63\ 659 = x$	0	-

Les calculs sont plus simples que les explications.

$$23\ 320 \cdot 10\ 103 = 235\ 601\ 960 \quad 3\ 701 \cdot 63\ 659 = 235\ 601\ 959$$

$$23\ 320 \cdot 10\ 103 - 3\ 701 \cdot 63\ 659 = 1$$

2.2.2. Inversion (mod n)

5 L'algorithme d'Euclide calcule aussi l'inverse (mod x). Lorsque y est positif, que x est plus grand que y et que x et y sont premiers entre eux, c'est-à-dire, $C_L = \text{pgcd}(x, y) = 1$, les notations « $y^{-1} \pmod{x}$ » et « $1/y \pmod{x}$ » ont un sens. Bien entendu, la suite $\{A\}$ est alors inutile.

Lorsque L est impair, l'inverse de $y \pmod{x}$ est égal à B_L .

10 Lorsque L est pair, l'inverse de $y \pmod{x}$ est égal à $x - B_L$.

Dans l'exemple ci-dessus, 23 320 est l'inverse de 10 103 (mod 63 659).

2.2.3. Méthode des restes chinois

15 Lorsque x et y sont deux entiers positifs premiers entre eux, les calculs suivants transforment une représentation à une composante (mod $x.y$) en une représentation à deux composantes (mod x) et (mod y).

$$a_x \equiv a_{x,y} \pmod{x} \text{ et } a_y \equiv a_{x,y} \pmod{y}$$

20 Voyons maintenant comment réaliser l'opération inverse, c'est-à-dire, comment calculer la représentation à une composante (mod $x.y$) connaissant la représentation à deux composantes (mod x) et (mod y). La technique décrite ci-dessous est connue comme la « méthode des restes chinois. »

Supposons x plus grand que y . Tout d'abord, réduisons $x \pmod{y}$, puis, inversons le résultat (mod y). Ce calcul est généralement fait à l'avance et le nombre λ est stocké dans le dispositif de calcul. Le nombre λ est un « paramètre des restes chinois. »

$$25 \quad \lambda = \{x \pmod{y}\}^{-1} \pmod{y}$$

Ensuite, réduisons la composante $a_x \pmod{y}$.

$$a'_x = a_x \pmod{y}$$

Le résultat cherché s'obtient alors par l'une des deux formules suivantes.

Lorsque a_y est supérieur ou égal à a'_x ,

$$a_{xy} \equiv \{\lambda \cdot (a_y - a'_x) \pmod{y}\} \cdot x + a_x$$

5 Lorsque a_y est inférieur à a'_x ,

$$a_{xy} \equiv \{\lambda \cdot (a_y + y - a'_x) \pmod{y}\} \cdot x + a_x$$

2.3. Calcul du symbole de Jacobi

Le calcul du symbole de Jacobi d'un entier positif k par rapport à un entier positif impair n plus grand que k se déroule selon la procédure suivante qui
10 utilise cinq variables appelée x , y , z , e et J . Cette procédure n'utilise pas la décomposition de n en facteurs premiers.

- La variable x est positive et impaire, strictement décroissante à partir de la valeur initiale n .
- La variable y est positive et inférieure à x , strictement décroissante à
15 partir de la valeur initiale k .
- La variable z est positive, impaire et inférieure à y .
- La variable e est l'exposant du facteur 2 extrait de y . Seule sa parité doit être évaluée.
- La variable J vaut +1 ou -1 en partant de la valeur initiale +1.

20 **Calcul pratique de $(k | n)$ avec k positif et n impair et plus grand que k**

1. Donner à x la valeur n ; donner à y la valeur k ; donner à J la valeur +1.

2. Décomposer y en $z \cdot 2^e$ où z est impair et positif et e positif ou nul.

$$(y | x) = (z \cdot 2^e | x) = (z | x) \cdot (2 | x)^e$$

⇒ Si e est impair et si $x = 3$ ou $5 \pmod{8}$, changer le signe de J .

3. Appliquer la loi de réciprocité quadratique sur z et x qui sont tous deux impairs.

$$(z | x) = (x | z) \cdot (-1)^{(x-1)(z-1)/4}$$

⇒ Si x et $z = 3 \pmod{4}$, changer le signe de J .

4. Réduire x qui est toujours plus grand que z .

⇒ Remplacer y par $x \pmod{z}$.

⇒ Remplacer x par z .

5

5. Si x est plus grand que 1, revenir à l'étape 2.

Si x est égal à 1, alors le symbole de Jacobi vaut J et les deux nombres k et n sont premiers entre eux.

Si x est nul, alors le symbole de Jacobi est nul et le pgcd de k et n est égal à z .

10

Exemple. Calculer $(10\ 103 \mid 63\ 659)$, c'est-à-dire, $(2777 \mid F8AB)$ en notation hexadécimale.

On retrouve les divisions successives de l'algorithme d'Euclide et le calcul du pgcd. Le décalage de ligne matérialise l'extraction du facteur 2. Le symbole « * » matérialise le changement de signe de J .

15

q	C	$C \pmod{8}$	J change
-	$63\ 659 = x$	3	
6	$10\ 103 = y$	7	*
3	3 041	1	
-	980	4	
12	245	5	
2	101	5	
2	43	3	
2	15	7	*
1	13	5	
-	2	2	*
13	1	1	

Par conséquent, $(10\ 103 \mid 63\ 659) = -1$.

2.4. Carré et racine carrée dans Q_n

Dans ce paragraphe, le module n est le produit de deux facteurs premiers p_1 et p_2 congrus à 3 (mod 4). Dans ce cas, $(p_1+1)/4$ et $(p_2+1)/4$ sont des nombres entiers.

Définissons la notation « (mod* n) ». Cette opération consiste à calculer normalement le résultat $x \pmod{n}$, puis, à garder x ou $n-x$, le plus petit des deux, comme résultat final.

Lorsque le module n est le produit de deux facteurs premiers p_1 et p_2 congrus à 3 (mod 4), définissons la notation « Q_n ». C'est l'ensemble des éléments de l'anneau des entiers (mod n) qui sont plus petits que $n/2$ et dont le symbole de Jacobi par rapport à n vaut +1. L'ensemble Q_n a une structure d'anneau.

Considérons une première transformation définie par « élever un élément x de Q_n au carré (mod* n) ». Le résultat y appartient également à Q_n .

$$y \equiv x^2 \pmod{*n}$$

Considérons une deuxième transformation définie par « élever y à la puissance $(p_1+1)/4 \pmod{p_1}$ », puis, « élever y à la puissance $(p_2+1)/4 \pmod{p_2}$ », avant d'utiliser la méthode des restes chinois pour établir le résultat $z \pmod{*n}$. Lorsque p_1 est plus petit que p_2 , les calculs sont très précisément les suivants.

$$y_1 \equiv y \pmod{p_1}; \quad z_1 \equiv y_1^{(p_1+1)/4} \pmod{p_1}$$

$$y_2 \equiv y \pmod{p_2}; \quad z_2 \equiv y_2^{(p_2+1)/4} \pmod{p_2}$$

$$z' \equiv z_2 \pmod{p_1}; \quad \text{Si } z_1 \geq z', \quad z'' = z_1 - z'; \quad \text{Sinon, } z'' = z_1 + p_1 - z'$$

$$\lambda \equiv \{p_2 \pmod{p_1}\}^{-1} \pmod{p_1};$$

$$z_{1,2} \equiv \{\lambda \cdot z'' \pmod{p_1}\} \cdot p_2 + z_2; \quad z \equiv z_{1,2} \pmod{*n}$$

Ces deux transformations sont inverses l'une de l'autre. Leur produit est l'identité parce que le résultat z rétablit le nombre x de départ. Ce sont deux permutations, inverses l'une de l'autre, des éléments de Q_n .

La première permutation calcule « le carré y dans Q_n de l'élément x de Q_n ».

La deuxième transformation calcule donc « la racine carrée x dans Q_n de l'élément y de Q_n ».

5 Par la suite, on aura besoin de la « k ième racine carrée de y dans Q_n , » c'est-à-dire, de la solution x dans Q_n à l'équation :

$$y \equiv x^{2^k} \pmod{*n}$$

Plutôt que d'extraire k racines carrées de rang dans Q_n , il vaut mieux procéder « globalement » de la manière suivante. Cette remarque fut faite en son temps par Oded Goldreich.

$$\begin{aligned} y_1 &\equiv y \pmod{p_1}; \quad z = (p_1 + 1)/4; \quad t \equiv z^k \pmod{p_1 - 1}; \quad x_1 \equiv y_1^t \pmod{p_1} \\ y_2 &\equiv y \pmod{p_2}; \quad z = (p_2 + 1)/4; \quad t \equiv z^k \pmod{p_2 - 1}; \quad x_2 \equiv y_2^t \pmod{p_2} \\ x' &\equiv x_2 \pmod{p_1}; \quad \text{Si } x_1 \geq x', \quad x'' = x_1 - x'; \quad \text{Sinon, } x'' = x_1 + p_1 - x' \end{aligned}$$

$$\lambda \equiv \{p_2 \pmod{p_1}\}^{-1} \pmod{p_1};$$

$$15 \quad x_{1,2} \equiv \{\lambda \cdot x'' \pmod{p_1}\} p_2 + x_2; \quad x \equiv x_{1,2} \pmod{*n}$$

2.5. Nombres de Williams et racine carrée de 4 dans Q_n

Hugh C. Williams a découvert l'intérêt cryptographique des modules n , produits de deux facteurs premiers p_1 et p_2 tels que p_1 soit congru à 3 (mod 8) et p_2 à 7 (mod 8).

20 Lorsque le module n est le produit de deux facteurs premiers p_1 et p_2 tels que p_1 soit congru à 3 (mod 8) et p_2 à 7 (mod 8), on obtient $(2 \mid p_1) = -1$ et $(2 \mid p_2) = +1$, c'est-à-dire que 2 est un résidu non quadratique (mod p_1) et un résidu quadratique (mod p_2); donc, ni 2 (mod n), ni -2 (mod n) n'appartiennent à Q_n .

25 Par la suite, α dénotera la racine carrée de 4 dans Q_n . Cette racine est représentée par les composantes : $\alpha_1 \equiv -2 \pmod{p_1}$ et $\alpha_2 \equiv 2 \pmod{p_2}$ ou bien par $\alpha_1 \equiv 2 \pmod{p_1}$ et $\alpha_2 \equiv -2 \pmod{p_2}$; c'est l'élément dont la représentation (mod n) est plus petite que $n/2$.

Il y a alors équivalence entre

la connaissance du nombre α et

la connaissance de la factorisation du module n .

Démonstration.

D'une part, étant donné α , le module n divise $\alpha^2 - 4$; mais le symbole de Jacobi de α par rapport à n vaut +1 alors que celui de 2 vaut -1 ; le module n ne divise donc ni $\alpha - 2$, ni $\alpha + 2$. Par conséquent, le facteur premier p_2 est le plus grand commun diviseur de n et $\alpha - 2$; le facteur premier p_1 est le plus grand commun diviseur de n et $\alpha + 2$.

D'autre part, étant donnés les facteurs premiers p_1 et p_2 , la racine carrée de 4 dans \mathbb{Q}_n est représentée par les composantes : $\alpha_1 \equiv -2 \pmod{p_1}$ et $\alpha_2 \equiv 2 \pmod{p_2}$, ou bien, $\alpha_1 \equiv 2 \pmod{p_1}$ et $\alpha_2 \equiv -2 \pmod{p_2}$. Selon les restes chinois, on reconstruit α .

Shafi Goldwasser, Silvio Micali et Ronald Rivest ont introduit la paire de fonctions $\{F_0; F_1\}$ sur \mathbb{Q}_n .

$$F_0(x) \equiv x^2 \pmod{*n} \text{ et } F_1(x) \equiv 4x^2 \pmod{*n}$$

Cette paire de fonctions permute les éléments de \mathbb{Q}_n .

Une « collision » est définie par deux éléments x et y de \mathbb{Q}_n tels que $F_0(x) = F_1(y)$. Connaître une collision équivaut à connaître les facteurs premiers du module n . La démonstration est semblable à la démonstration ci-dessus. Par conséquent, cette paire de permutations résiste aux collisions pour qui ne connaît pas les facteurs premiers p_1 et p_2 du module n .

Nous disposons donc de tous les ingrédients nécessaires à une démonstration de la connaissance de la factorisation d'un module public n sans en transférer la connaissance.

3. Charges de travail

La charge de travail pour « élever x à la puissance v ième \pmod{n} » dépend de la valeur et de la forme binaire de l'exposant v , de la taille de l'argument x et de la taille du module n . Dans le cadre de ce mémoire, l'exposant v est plus petit que le plus petit facteur premier du module n .

L'utilisation des facteurs premiers p_1, p_2, \dots d'un module n diminue la charge de travail pour calculer $(\text{mod } n)$. Plutôt que l'opération directe « élever x à la puissance v ième $(\text{mod } n)$ », on peut avantageusement élever x à la puissance v ième dans chacun des corps $\text{CG}(p_1), \text{CG}(p_2), \dots$ c'est-à-dire, $(\text{mod } p_1), (\text{mod } p_2), \dots$ puis, établir le résultat dans l'anneau Z_n , c'est-à-dire, $(\text{mod } n = p_1 \text{ fois } p_2 \text{ fois } \dots)$. Cette manière de procéder est appelée la « méthode des restes chinois. »

3.1. Multiplication et carré $(\text{mod } n)$

En pratique, avec des programmes optimisés, le rapport entre la charge de travail pour un « carré modulo » et la charge de travail pour une « multiplication modulo » est environ 0,75. Par exemple, sur le composant ST 16601 pour carte à puce, avec une horloge normalisée à 3,579545 MHz, le carré modulo pour 512 bits se fait en 150 ms et la multiplication modulo en 200 ms.

Pour effectuer une opération « multiplication modulo », on peut multiplier, puis, réduire : l'opération de multiplication demande à peu près autant d'effort que l'opération de réduction modulo.

La multiplication de deux nombres de 512 bits peut se ramener à des multiplications de nombres de 256 bits. Chaque nombre de 512 bits s'écrit alors $a+b.2^{256}$ où a et b sont des nombres de 256 bits. La multiplication de $a+b.2^{256}$ par $c+d.2^{256}$ amène à calculer les quatre produits $a.c, a.d, b.c$ et $b.d$. En doublant la longueur, on multiplie par quatre la charge de travail pour multiplier. Le carré de $a+b.2^{256}$ amène à calculer les deux carrés a^2, b^2 et le produit $a.b$. En doublant la longueur, on multiplie par trois la charge de travail pour élever au carré.

De même, la multiplication de deux nombres de 512 bits peut se ramener à des multiplications de nombres de 171 bits. Chaque nombre de 512 bits s'écrit alors $a+2^{171}.b+2^{342}.c$ où a, b et c sont des nombres de 171 bits. La multiplication de $a+2^{171}.b+2^{342}.c$ par $d+2^{171}.e+2^{342}.f$ amène à calculer neuf. En

doublant la longueur, on multiplie par neuf la charge de travail pour multiplier. Le carré de $a+2^{171}.b+2^{342}.c$ amène à calculer trois carrés et trois produits. En doublant la longueur, on multiplie par six la charge de travail pour élever au carré.

3.2. Elever x à la puissance v ième (mod n)

Prenons en exemple la valeur $v = 3$, puis, la valeur $v = 65537$.

Pour $v = 3$, c'est-à-dire, $2+1$, il faut élever l'argument au carré (mod n), puis, multiplier le résultat par l'argument (mod n).

Pour $v = 65\,537$, c'est-à-dire, $2^{16}+1$, il faut élever l'argument au carré (mod n) seize fois de rang, puis, multiplier le résultat par l'argument (mod n).

Dans le cadre de ce mémoire, l'exposant v est plus petit que le plus petit facteur premier du module n . Il n'y a donc pas de réduction de l'exposant v en fonction des différents facteurs premiers du module n . Par rapport au calcul direct de « élever x à la puissance v ième (mod n) » où l'argument x et le module n ont la même taille, la méthode des restes chinois divise la charge de travail

- par deux lorsque le module n a deux facteurs premiers p_1 et p_2 de même taille,

- par trois lorsque le module n a trois facteurs premiers p_1 , p_2 et p_3 de même taille,

et ainsi de suite.

On peut généraliser la méthode précédente ; ainsi, la procédure suivante calcule $x^v \pmod{n}$ pour un exposant $v = 2^i + v_{i-1}.2^{i-1} + \dots + v_1.2 + v_0$ où chaque bit de v_{i-1} à v_0 vaut 0 ou 1.

1. Donner à y la valeur x .

2. Répéter la séquence suivante pour k allant de $i-1$ à 0.

Remplacer y par $y^2 \pmod{n}$.

Si le bit v_k vaut 1, remplacer y par $x.y \pmod{n}$.

3. Le résultat cherché est y .

Selon la procédure précédente, le calcul peut se faire par $\log_2(v)$ carrés (mod n) entrelacés avec $h(v)$ multiplications (mod n). La notation $h(v)$ représente un de moins que le poids de Hamming de v , c'est-à-dire, que l'écriture de v en binaire comporte $h(v)+1$ bits à 1.

Pour un module n de 512 bits, cela signifie $\log_2(v)$ carrés (mod n sur 512 bits) et $h(v)$ multiplications (mod n sur 512 bits).

Pour un module n de 256 bits, cela signifie $\log_2(v)$ carrés (mod n sur 256 bits) et $h(v)$ multiplications (mod n sur 256 bits).

Pour un module n de 171 bits, cela signifie $\log_2(v)$ carrés (mod n sur 171 bits) et $h(v)$ multiplications (mod n sur 171 bits).

Deuxième partie : nouveau procédé

1. Exposé du nouveau procédé

Le procédé est destiné à prouver l'origine et l'intégrité d'un message numérique m , lequel message peut être vide. Ce procédé permet l'authentification d'entité, l'authentification de message ou la signature de message.

1.1. Paramètres

Le procédé met en œuvre un premier ensemble de nombres entiers, à savoir au moins deux facteurs premiers notés par p_1 p_2 p_3 ... Certains facteurs premiers peuvent apparaître plusieurs fois. Le produit des facteurs premiers forme un module public $n = p_1 \cdot p_2 (\cdot p_3 \dots)$.

un jeu de « paramètres des restes chinois » notés λ_a λ_b λ_c Il y a un paramètre de moins que de facteurs premiers.

Attention, il y a plusieurs jeux de paramètres « équivalents. » Supposons que

les grands nombres premiers sont rangés dans l'ordre croissant,

s'il y a trois nombres premiers, p_3 est plus petit que p_1 fois p_2 ,

s'il y a quatre nombres premiers, p_4 est plus petit que p_1 fois p_2 fois p_3 ,

et ainsi de suite.

Dans ce cas, voici un exemple de jeu de paramètres des restes chinois.

$$\lambda_a \equiv (p_2 \pmod{p_1})^{-1} \pmod{p_1}$$

$$\lambda_b \equiv ((p_1 \cdot p_2 \pmod{p_3})^{-1} \pmod{p_3})$$

$$5 \quad \lambda_c \equiv ((p_1 \cdot p_2 \cdot p_3 \pmod{p_4})^{-1} \pmod{p_4})$$

Et ainsi de suite.

Le procédé met en œuvre un deuxième ensemble de nombres entiers, à savoir, au moins un exposant public de vérification noté par v , et, pour chaque exposant v , au moins une paire de clés selon la présente invention comprenant une clé privée notée par Q et une clé publique notée par G . Une des deux relations suivantes lie chaque paire de clés selon la présente invention par les nombres v et n .

$$G \cdot Q^v \equiv 1 \pmod{n} \text{ ou bien } G \equiv Q^v \pmod{n}$$

En l'absence de toute ambiguïté, en particulier, s'il y a un seul exposant public de vérification v , on utilise la notation (G, Q) , puis, si besoin est, (GA, QA) , (GB, QB) , (GC, QC) , ...

Avec plusieurs exposants publics de vérification $v_x \ v_y \ v_z \dots$, on utilise en outre la notation (G_x, Q_x) , (G_y, Q_y) , ..., puis, si besoins est, (G_xA, Q_xA) , (G_xB, Q_xB) , ... (G_yA, Q_yA) , (G_yB, Q_yB) , ...

En pratique, chaque clé privée Q n'est jamais utilisée telle quelle.

On utilise uniquement un jeu de composantes $Q_1 \ Q_2 \ Q_3 \dots$, une composante par facteur premier.

$$Q_1 \equiv Q \pmod{p_1}; \quad Q_2 \equiv Q \pmod{p_2}; \quad Q_3 \equiv Q \pmod{p_3};$$

et ainsi de suite.

Par la méthode des restes chinois, on pourrait rétablir chaque clé privée Q à partir du jeu de composantes $Q_1 \ Q_2 \ Q_3 \dots$. En pratique, il n'y a jamais lieu de rétablir les clés privées Q .

$$Q'_a \equiv Q_2 \pmod{p_1}; ;$$

$$\text{Si } Q_1 \geq Q'_a, \quad Q''_a = Q_1 - Q'_a; \text{ Sinon, } Q''_a = Q_1 + p_1 - Q'_a;$$

$$Q_{1,2} \equiv \{\lambda_a \cdot Q_a'' \pmod{p_1}\} p_2 + Q_2;$$

$$Q_b' \equiv Q_{1,2} \pmod{p_3};$$

Si $Q_3 \geq Q_b'$, $Q_b'' = Q_3 - Q_b'$; Sinon, $Q_b'' = Q_3 + p_3 - Q_b'$;

$$Q_{1,2,3} \equiv \{\lambda_b \cdot Q_b'' \pmod{p_3}\} p_1 \cdot p_2 + Q_{1,2};$$

5

Et ainsi de suite. Q est égal à $Q_{1,2,3}, \dots$

1.1.1. Paire de clés selon la présente invention conférant une sécurité équivalente à la connaissance de la clé privée Q

Les composantes Q_1 Q_2 Q_3 ... sont des nombres pris au hasard tels que $0 < Q_1 < p_1$, $0 < Q_2 < p_2$, $0 < Q_3 < p_3$, ... Il y a une composante par facteur premier. En pratique, pour réduire la charge de travail, on choisit des composantes Q_i « courtes », c'est-à-dire, de l'ordre de grandeur de la racine troisième ou quatrième du facteur premier p_i .

10

Note. L'ensemble de ces composantes représente une clé privée Q . La clé privée Q n'est jamais utilisée telle quelle.

15

$$Q_a' \equiv Q_2 \pmod{p_1}; ;$$

Si $Q_1 \geq Q_a'$, $Q_a'' = Q_1 - Q_a'$; Sinon, $Q_a'' = Q_1 + p_1 - Q_a'$;

$$Q_{1,2} \equiv \{\lambda_a \cdot Q_a'' \pmod{p_1}\} p_2 + Q_2;$$

$$Q_b' \equiv Q_{1,2} \pmod{p_3};$$

Si $Q_3 \geq Q_b'$, $Q_b'' = Q_3 - Q_b'$; Sinon, $Q_b'' = Q_3 + p_3 - Q_b'$;

20

$$Q_{1,2,3} \equiv \{\lambda_b \cdot Q_b'' \pmod{p_3}\} p_1 \cdot p_2 + Q_{1,2};$$

Et ainsi de suite. Q est égal à $Q_{1,2,3}, \dots$

La clé publique G est la puissance v ième de $Q \pmod{n}$ ou bien son inverse \pmod{n} .

$$G \equiv Q^v \pmod{n} \quad \text{ou bien} \quad G \equiv \{Q^v \pmod{n}\}^{-1} \pmod{n}$$

25

Note. En pratique, pour calculer le nombre G , on élève chaque nombre Q_i à la puissance v ième $\pmod{p_i}$, ..., puis, on utilise la méthode des restes chinois pour établir le résultat \pmod{n} ou son inverse \pmod{n} .

$$G_1 \equiv Q_1^v \pmod{p_1};$$

$$\begin{aligned}
& G_2 \equiv Q_2^v \pmod{p_2}; \quad G_a' \equiv G_2 \pmod{p_1}; \\
& \text{Si } G_1 \geq G_a', \quad G_a'' = G_1 - G_a'; \quad \text{Sinon, } G_a'' = G_1 + p_1 - G_a'; \\
& G_{1,2} \equiv \{\lambda_a \cdot G_a'' \pmod{p_1}\} p_2 + G_2; \quad G_b' \equiv G_{1,2} \pmod{p_3}; \\
& \quad G_3 \equiv Q_3^v \pmod{p_3} \\
& \text{Si } G_3 \geq G_b', \quad G_b'' = G_3 - G_b'; \quad \text{Sinon, } G_b'' = G_3 + p_3 - G_b'; \\
& \quad G_{1,2,3} \equiv \{\lambda_b \cdot G_b'' \pmod{p_3}\} p_1 \cdot p_2 + G_{1,2};
\end{aligned}$$

Et ainsi de suite. G est égal à $G_{1,2,3,\dots}$ ou bien, à son inverse \pmod{n} .

Lorsque le nombre entier v est premier, on assure la propriété de sécurité annoncée.

1.1.2. Paire de clés selon la présente invention conférant une sécurité équivalente à la connaissance de la factorisation de n

L'exposant public de vérification v est égal à 2^k . Le nombre entier k est un paramètre de sécurité plus grand que 1. La valeur $k = 1$ est interdite.

Chaque nombre g est un entier inférieur au plus petit facteur premier. En outre, pour au moins un facteur premier p , l'équation $x^2 \equiv g \pmod{p}$ n'a pas de solution en x dans $\text{CG}(p)$ et pour au moins un facteur q l'équation $x^2 \equiv -g \pmod{q}$ n'a pas de solution en x dans $\text{CG}(q)$. Cette construction assure que les deux équations $x^2 \equiv g \pmod{n}$ et $x^2 \equiv -g \pmod{n}$ n'ont pas de solution en x dans l'anneau des entiers modulo n , c'est-à-dire que les nombres g et $-g$ sont deux résidus non quadratiques \pmod{n} .

Note. En pratique, on utilise pour g les nombres 2, 3, 5, 6, ... en éliminant bien sûr les carrés tels que 4, 9, ...

Note. Il n'est pas recommandé d'utiliser 6 comme nombre de base en même temps que 2 et 3 parce qu'ils se combinent par multiplication. On dit qu'ils ne sont pas « indépendants. » Il vaut mieux utiliser 2 et 3 comme nombres de base et retrouver 6 comme le produit de 2 et 3.

Pour chaque nombre g , la clé publique G est égale à g^2 .

Pour chaque nombre g , chaque composante Q_1, Q_2, Q_3, \dots est la k ième racine carrée de G dans $CG(p)$ qui est un résidu quadratique dans $CG(p)$. Il y a une composante par facteur premier.

Exemple de calcul de la k ième racine carrée quadratique de G dans $CG(p)$

5 On pourra utilement consulter l'appendice 3, « *Quadratic Residues* », pp. 278-288, dans l'ouvrage « *Prime Numbers and Computer Methods for Factorization* », Hans Riesel, Birkhäuser, Boston, Basel, Stuttgart, 1985.

10 Pour chaque facteur premier p congru à 3 (mod 4), on élève k fois de rang G à la puissance $(p+1)/4$ pour obtenir la k ième racine carrée quadratique de G dans le corps $CG(p)$; puis, on inverse ou non le résultat (mod p) pour obtenir la composante Q_i pour le facteur premier p_i .

Note. Plutôt que d'extraire k racines carrées successivement, on peut procéder de manière globale.

15
$$x = (p+1)/4; y \equiv x^k \pmod{p-1}; z = p-1-y; Q_p \equiv G^z \pmod{p};$$

par conséquent, p divise $G \cdot Q_p^{2^k} - 1$.

ou bien,

$$x = (p+1)/4; y \equiv x^k \pmod{p-1}; z = y; Q_p \equiv G^z \pmod{p};$$

par conséquent, p divise $Q_p^{2^k} - G$.

20 Pour chaque facteur premier p congru à 1 (mod 4), on utilise les suites de Lucas pour extraire les racines carrées successives, jusqu'à obtenir la k ième racine carrée de G dans le corps $CG(p)$, avant d'inverser ou non le résultat (mod p) pour obtenir la composante Q_i pour le facteur premier p_i .

Par conséquent, p divise $G \cdot Q_p^{2^k} - 1$ ou bien, $Q_p^{2^k} - G$.

25 Les clés G et Q sont deux résidus quadratiques (mod n). La paire de clés selon la présente invention vérifie l'une des deux relations suivantes.

$$G \cdot Q^{2^k} \equiv 1 \pmod{n} \quad \text{ou bien,} \quad Q^{2^k} \equiv G \pmod{n}$$

Par conséquent, dans l'anneau des entiers modulo n , le $k-1$ ième carré de chaque clé privée Q ou son inverse (mod n) est une racine carrée non

triviale de la clé publique $G = g^2$. Appelons q cette racine carrée de $G \pmod{n}$ qui n'est ni g ni $-g$. Par conséquent, n qui divise $q^2 - g^2$ ne divise ni $q - g$ ni $q + g$. Ainsi, le module n se scinde en deux facteurs non triviaux : le pgcd de n et de $q - g$ et le pgcd de n et de $q + g$. Par conséquent, pour n'importe quelle

5 clé privée Q , la connaissance de n'importe laquelle des k valeurs $\{Q, Q^2, Q^4, \dots \text{ jusqu'au } k-1 \text{ ième carré de } Q \pmod{n}\}$ révèle une factorisation non triviale du module n .

Contraintes induites par les nombres de base sur les facteurs premiers

On peut utilement consulter le chapitre 3, « *Quadratic Residues* », pp. 35-46, dans l'ouvrage « *Introduction to Number Theory* », Hua Loo Keng, Springer Verlag, Berlin, Heidelberg, 1982.

10

❖ $(2 \mid p) = +1$ lorsque p est congru à $\pm 1 \pmod{8}$.

$(2 \mid p) = -1$ lorsque p est congru à $\pm 3 \pmod{8}$.

Pour utiliser $g = 2$, c'est-à-dire, la clé publique $G = 4$, il suffit qu'un

15 facteur premier soit congru à $\pm 3 \pmod{8}$. Alors, le nombre 2 est un résidu non quadratique modulo n .

❖ $(3 \mid p) = +1$ lorsque p est congru à $\pm 1 \pmod{12}$.

$(3 \mid p) = -1$ lorsque p est congru à $\pm 5 \pmod{12}$.

Pour utiliser $g = 3$, c'est-à-dire, la clé publique $G = 9$, il suffit qu'un

20 facteur premier soit congru à $\pm 5 \pmod{12}$. Alors, le nombre 3 est un résidu non quadratique modulo n .

❖ Le nombre $g = 4$ est un carré ; il n'est donc pas utilisé.

❖ $(5 \mid p) = +1$ lorsque p est congru à $\pm 1 \pmod{5}$.

$(5 \mid p) = -1$ lorsque p est congru à $\pm 2 \pmod{5}$.

Pour utiliser $g = 5$, c'est-à-dire, la clé publique $G = 25$, il suffit qu'un

25 facteur premier soit congru à $\pm 2 \pmod{5}$. Alors, le nombre 5 est un résidu non quadratique modulo n .

❖ $(6 \mid p) = +1$ lorsque p est congru à ± 1 ou $\pm 5 \pmod{24}$.

$(6 \mid p) = -1$ lorsque p est congru à ± 7 ou $\pm 11 \pmod{24}$.

Pour utiliser $g = 6$, c'est-à-dire, la clé publique $G = 36$, il suffit qu'un facteur premier soit congru à ± 7 ou $\pm 11 \pmod{24}$. Alors, le nombre 6 est un résidu non quadratique modulo n .

❖ $(7 \mid p) = +1$ lorsque p est congru à $\pm 1, \pm 3$ ou $\pm 9 \pmod{28}$.

5 $(7 \mid p) = -1$ lorsque p est congru à $\pm 5, \pm 11$ ou $\pm 13 \pmod{28}$.

Pour utiliser $g = 7$, c'est-à-dire, la clé publique $G = 49$, il suffit qu'un facteur premier soit congru à $\pm 2 \pmod{5}$. Alors, le nombre 7 est un résidu non quadratique modulo n .

10 **Note.** Tous les témoins peuvent utiliser le même jeu de clés publiques GA, GB, GC, GD, \dots , par exemple, 4, 9, 25 et 49, moyennant des contraintes élémentaires sur la sélection des facteurs premiers. Ces contraintes sont pratiquement gratuites lorsqu'elles sont intégrées aux procédures de production des facteurs premiers.

1.1.3. Généralisation de la structure précédente

15 Le nombre a est un nombre impair. Il doit diviser au moins un facteur premier moins un.

Note. En pratique, on donne au nombre a les valeurs des nombres premiers à partir de 3, soit : 3, 5, 7, 11, ...

20 L'exposant public de vérification v est égal à a^k . Le nombre entier k est un paramètre de sécurité plus grand que 1. La valeur $k = 1$ est interdite.

Chaque nombre g est un entier inférieur au plus petit facteur premier. En outre, pour au moins un facteur premier p tel que a divise $p-1$, l'équation $x^a \equiv g \pmod{p}$ n'a pas de racine en x dans $CG(p)$.

25 **Note.** Cette construction généralise les résidus non quadratiques \pmod{n} . Par exemple, dans le cas $a = 3$, on dit que le nombre g est un résidu non cubique \pmod{n} . Dans le cas général, on parle de résidu non a dique \pmod{n} .

Note. En pratique, on donne au nombre g les valeurs 2, 3, 4, 5, ... en éliminant les puissances a ièmes.

Pour chaque nombre g , la clé publique G est égale à g^a .

Pour chaque nombre g , chaque composante $Q_1 Q_2 Q_3 \dots$ est la k ième racine a ième de G dans $CG(p)$ qui est un résidu a dique dans $CG(p)$. Il y a une composante par facteur premier.

5 Exemple de calcul de la k ième racine troisième de G dans $CG(p)$ qui est un résidu cubique dans $CG(p)$.

Pour chaque facteur premier p congru à 2 (mod 3), on élève k fois de rang G à la puissance $(p-2)/3$ pour obtenir la k ième racine a ième de G dans le corps $CG(p)$; puis, on inverse ou non le résultat (mod p) pour obtenir la
10 composante Q_i pour le facteur premier p_i .

Note. On peut procéder de manière globale pour accéder directement au résultat cherché.

$$x = (p-2)/3; y \equiv x^k \pmod{p-1}; z = y; Q_p \equiv G^z \pmod{p};$$

$$\text{par conséquent, } p \text{ divise } Q_p^{3^k} - G.$$

15 $x = (p-2)/3; y \equiv x^k \pmod{p-1}; z = p-1-y; Q_p \equiv G^z \pmod{p};$

$$\text{par conséquent, } p \text{ divise } G \cdot Q_p^{3^k} - 1.$$

Pour chaque facteur premier p congru à 1 (mod 3),

$$p \text{ divise } G \cdot Q_p^{3^k} - 1 \text{ ou bien } Q_p^{3^k} - G.$$

1.2. Entités

20 Le procédé met en œuvre les trois entités suivantes.

Une première entité témoigne ; c'est le **témoin**. Il dispose d'un exposant public de vérification $v = 2^k$. En fonction des compromis retenus entre charge de travail et volume de données à stocker, le témoin stocke encore d'autres nombres :

25 - ou bien les j facteurs premiers $p_1 p_2 p_3 \dots$ et les l clés publiques $GA GB \dots$; à chaque appel, le témoin doit alors reconstituer les l clés privées $QA QB \dots$ selon le paramètre k à partir des l clés publiques $GA GB \dots$ et des j facteurs premiers $p_1 p_2 p_3 \dots$;

- ou bien, le module n et les l clés privées $QA\ QB\ \dots$; le témoin ne fait alors appel ni aux facteurs premiers ni aux restes chinois ;
- ou bien un ensemble de $j.(l+2)-1$ nombres privés de tailles voisines pour utiliser les facteurs premiers et les restes chinois :

- 5
- j facteurs premiers $p_1\ p_2\ p_3\ \dots$,
 - $j-1$ paramètres des restes chinois $\lambda_1\ \lambda_2\ \dots$,
 - $j.l$ composantes de clés privées : $QA_1\ QA_2\ \dots\ QB_1\ QB_2\ \dots$

10 Une deuxième entité pilote le témoin ; c'est le **pilote**. Il dispose d'un certificat $Cert(Id, n)$ liant le module n à une identité Id . Il connaît un message m . S'il s'agit d'une authentification dynamique, c'est-à-dire, d'une preuve interactive de connaissance, il est encore appelé **démonstrateur**. En cas d'authentification d'entité, le démonstrateur n'a pratiquement rien à faire. En cas d'authentification de message, le démonstrateur dispose d'une fonction de hachage f . S'il s'agit d'une signature numérique de message,

15 c'est-à-dire, d'une preuve non interactive de connaissance, le pilote est encore appelé **signataire** ; le signataire dispose de l'exposant public de vérification v et d'une fonction de hachage f .

20 Une troisième entité vérifie ; c'est le **contrôleur**. Selon le cas, le contrôleur vérifie l'authentification ou la signature ; il dispose d'un module public N pour ouvrir les certificats afin d'établir une identité Id et un module n , de l'exposant public de vérification $v = 2^k$, des l clés publiques GA, GB, \dots et de la fonction de hachage f .

25 **Note.** Chaque jeu de composantes $Q_1\ Q_2\ Q_3\ \dots$ représente une clé privée Q . Chaque paire de clés selon la présente invention est liée aux nombres v et n par l'une des deux relations suivantes.

$$G.Q^v \equiv 1 \pmod{n} \text{ ou bien } G \equiv Q^v \pmod{n}$$

En termes de charge de travail du témoin, la solution optimale consiste à utiliser les facteurs premiers, les paramètres des restes chinois et les composantes des clés privées. Chaque clé privée Q est construite, puis,

stockée et utilisée sous la forme de composantes, Q_1, Q_2, \dots une composante par facteur premier, p_1, p_2, \dots . Les clés privées Q n'apparaissent alors jamais et le témoin n'utilise pas non plus les clés publiques G .

En termes de charge de travail du contrôleur, la solution optimale consiste à utiliser pour G une valeur qui soit la plus petite possible. Les valeurs sur un seul quartet ou un seul octet sont particulièrement conseillées. En pratique, on utilise pour ga, gb, \dots les premiers nombres premiers : 2, 3, 5, 7, 11,

Dans la présentation qui suit le témoin utilise les facteurs premiers et les restes chinois. Le témoin peut s'en abstenir, ce qui affecte simplement et seulement les actions du témoin. Le protocole GQ2 déroule les étapes suivantes permettant au contrôleur de vérifier l'origine et l'intégrité d'un message m .

- L'authentification dynamique est une preuve interactive.
- La signature numérique est une preuve non interactive.

1.3. Etapes

Le procédé comporte les étapes suivantes.

Etape 1. Engagement du témoin

• A chaque appel, pour chaque exposant public de vérification vx, vy, vz, \dots , le témoin tire au hasard et en privé au moins un jeu de nombres entiers : pour chaque facteur premier p_i , chaque jeu comporte un nombre entier r_i positif et plus petit que p_i . Ces nombres entiers sont ensuite appelés les aléas r_1, r_2, r_3, \dots

$$0 < r_1 < p_1; \quad 0 < r_2 < p_2; \quad 0 < r_3 < p_3; \quad \dots$$

• Pour chaque exposant public de vérification vx, vy, vz, \dots , et pour chaque facteur premier p_i , le témoin élève chaque aléa r_i à la puissance v ième (mod p_i).

$$R_1 \equiv r_1^v \pmod{p_1}; \quad R_2 \equiv r_2^v \pmod{p_2}; \quad R_3 \equiv r_3^v \pmod{p_3}; \quad \dots$$

• Puis, le témoin établit chaque engagement $R \pmod{n}$ selon la méthode des restes chinois.

$$R_a' \equiv R_2 \pmod{p_1};$$

Si $R_1 \geq R_a'$, $R_a'' = R_1 - R_a'$; Sinon, $R_a'' = R_1 + p_1 - R_a'$;

$$R_{1,2} \equiv \{\lambda_a \cdot R_a'' \pmod{p_1}\} \cdot p_2 + R_2; \quad R_b' \equiv R_{1,2} \pmod{p_3};$$

Si $R_3 \geq R_b'$, $R_b'' = R_3 - R_b'$; Sinon, $R_b'' = R_3 + p_3 - R_b'$;

$$5 \quad R_{1,2,3} \equiv \{\lambda_b \cdot R_b'' \pmod{p_3}\} \cdot p_1 \cdot p_2 + R_{1,2};$$

Et ainsi de suite. R est égal à $R_{1,2,3} \dots$

Pour chaque exposant public de vérification $v_x \ v_y \ v_z \dots$, il y a autant d'engagements R que de jeux d'aléas $r_1 \ r_2 \ r_3 \dots$

Etape 2. Défi au témoin

10 En cas d'authentification d'entité,

le démonstrateur transmet tout ou partie de chaque engagement R au contrôleur ;

après avoir reçu tout ou partie de chaque engagement R , le contrôleur produit au moins une séquence de nombres de 0 à $v-1$ pris au hasard.

15 En cas d'authentification de message,

le démonstrateur applique une fonction de hachage f ayant comme arguments le message m et chaque engagement R pour obtenir un jeton T à transmettre au contrôleur,

après avoir reçu le jeton T , le contrôleur produit au moins une séquence de
20 nombres de 0 à $v-1$ pris au hasard.

En cas de signature numérique de message, le signataire applique une fonction de hachage f ayant comme arguments le message m et chaque engagement R pour obtenir au moins une séquence de nombres de 0 à $v-1$.

25 Dans les trois cas, pour chaque exposant public de vérification $v_x \ v_y \ v_z \dots$, chaque séquence comporte autant de nombres de 0 à $v-1$ qu'il y a de paires de clés selon la présente invention ; dans chaque séquence, les nombres sont notés par dA, dB, \dots . Chaque séquence de nombres de 0 à $v-1$ est ensuite appelée défi d . Pour chaque exposant public de vérification $v_x \ v_y \ v_z \dots$, il y a autant de défis d que d'engagements R .

Etape 3. Réponse du témoin au défi

- Pour chaque exposant public de vérification $vx \quad vy \quad vz \dots$, pour chaque facteur premier p_i , le témoin calcule

la puissance dA ième de la composante $QA_i \pmod{p_i}$,

5 la puissance dB ième de la composante $QB_i \pmod{p_i}$,

...

le produit des résultats précédents par l'aléa $r_i \pmod{p_i}$;

$$D_1 \equiv r_1 \cdot QA_1^{dA} \cdot QB_1^{dB} \dots \pmod{p_1}; \quad D_2 \equiv r_2 \cdot QA_2^{dA} \cdot QB_2^{dB} \dots \pmod{p_2};$$

$$D_3 \equiv r_3 \cdot QA_3^{dA} \cdot QB_3^{dB} \dots \pmod{p_3};$$

- 10 • Puis, pour chaque exposant public de vérification $vx \quad vy \quad vz \dots$, le témoin établit au moins une réponse $D \pmod{n}$ selon la méthode des restes chinois.

$$D'_a \equiv D_2 \pmod{p_1};$$

Si $D_1 \geq D'_a$, $D''_a = D_1 - D'_a$; Sinon, $D''_a = D_1 + p_1 - D'_a$;

$$D_{1,2} \equiv \{\lambda_a \cdot D''_a \pmod{p_1}\} p_2 + D_2;$$

15 $D'_b \equiv D_{1,2} \pmod{p_3};$

Si $D_3 \geq D'_b$, $D''_b = D_3 - D'_b$; Sinon, $D''_b = D_3 + p_3 - D'_b$;

$$D_{1,2,3} \equiv \{\lambda_b \cdot D''_b \pmod{p_3}\} p_1 \cdot p_2 + D_{1,2};$$

Et ainsi de suite. D est égal à $D_{1,2,3} \dots$

20 Pour chaque exposant public de vérification $vx \quad vy \quad vz \dots$, il y a autant de réponses D que de défis d .

Note. Chaque appel au témoin se traduit à l'interface par autant de triplets $\{R, d, D\}$ que de jeux d'aléas $r_1 \quad r_2 \quad r_3 \dots$. Remarquons qu'en élevant la réponse D à la puissance v ième \pmod{n} , on doit retrouver l'engagement R divisé ou multiplié, selon l'équation retenue pour lier les paires de clés selon la présente invention aux nombres v et n , par la puissance dA ième de

25 GA , la puissance dB ième de GB , ... Par conséquent, chaque triplet $\{R, d, D\}$ doit vérifier l'une des deux relations suivantes.

$$R \equiv GA^{dA} \cdot GB^{dB} \cdot \dots \cdot D^v \pmod{n};$$

$$\text{ou bien } R \cdot GA^{dA} \cdot GB^{dB} \cdot \dots \equiv D^v \pmod{n};$$

Etape 4. Données destinées au contrôleur

En cas d'authentification d'entité ou de message, le démonstrateur transmet chaque réponse D au contrôleur.

En cas de signature numérique de message, le signataire transmet un message signé au contrôleur. Le message signé comprend le message m , ainsi que :

- * chaque défi d ou chaque engagement R ,
- * chaque réponse D .

Etape 5. Vérification exercée par le contrôleur

Note. On aurait pu tester ici le symbole de Jacobi de chaque réponse, à condition d'avoir forcé le symbole de l'aléa à l'étape 1. Cependant, il vaut mieux « laisser tomber les symboles ». Il est bien plus économique d'accepter de perdre un bit de défi.

Note. L'une des deux relations suivantes reconstruit un engagement noté par R' .

$$R' \equiv (GA^{dA} . GB^{dB} . \dots) D^v \pmod{n};$$

$$\text{ou bien } R' \equiv D^v / (GA^{dA} . GB^{dB} . \dots) \pmod{n};$$

En cas d'authentification d'entité, le contrôleur doit appliquer la formule appropriée pour reconstruire chaque engagement R' : aucun ne doit être nul. Chaque engagement reconstruit R' doit reproduire l'intégralité des données transmises à l'étape 2, c'est-à-dire, tout ou partie de chaque engagement R . Lorsque toutes les conditions sont remplies, l'authentification d'entité est réussie.

En cas d'authentification de message, le contrôleur doit appliquer la formule appropriée pour reconstruire chaque engagement R' : aucun ne doit être nul. Puis, il doit appliquer la fonction de hachage f ayant comme arguments le message m et chaque engagement reconstruit R' pour reconstruire le jeton T' . Le jeton reconstruit T' doit être identique au jeton T .

de l'étape 2. Lorsque toutes les conditions sont remplies, l'authentification de message est réussie.

En cas de signature numérique de message, selon le cas,

- le contrôleur doit appliquer la formule appropriée pour reconstruire chaque engagement R' : aucun ne doit être nul. Puis, il doit appliquer la fonction de hachage f ayant comme arguments le message m et chaque engagement reconstruit R' pour reconstruire chaque défi d' . Chaque défi reconstruit d' doit être identique au défi d figurant dans le message signé. Lorsque toutes les conditions sont remplies, la signature est correcte.
- le contrôleur doit appliquer la fonction de hachage f ayant comme arguments le message m et chaque engagement R figurant dans le message signé pour reconstruire chaque défi d' . Puis, il doit appliquer la formule appropriée pour contrôler la cohérence de chaque triplet $\{R, d', D\}$. Chaque triplet doit être cohérent. Lorsque toutes les conditions sont remplies, la signature numérique est correcte.

2. Triplets

Chaque appel au témoin se traduit par une collection de triplets à l'interface du témoin. Chaque triplet $\{R, d, D\}$ comprend un engagement R , un défi d et une réponse D . Il y a deux manières de produire des triplets : une manière de produire en privé et une manière de produire en public.

- Le témoin produit en privé selon la chronologie suivante : à chaque appel, il fixe d'abord un nouveau jeu d'aléas qu'il transforme en un engagement R , puis, il produit la réponse D à n'importe quel défi d de 0 à $v-1$.
- N'importe qui peut produire en public selon la chronologie suivante : quel que soit le défi d de 0 à $v-1$, n'importe qui peut compléter le

triplet à partir de n'importe quelle réponse D en établissant l'engagement R grâce aux nombres publics G , v et n .

3. Tenailles

Par définition, deux triplets sont « en tenaille » lorsqu'ils sont constitués des deux réponses D et E à deux défis d et e pour le même engagement R , c'est-à-dire, $\{R, d, D\}$ et $\{R, e, E\}$.

A chaque appel, le témoin est en position de produire des triplets en tenaille : il lui suffirait de réutiliser un jeu d'aléas. Mais il se garde bien des tenailles : en tirant au hasard un jeu d'aléas à chaque appel, il utilise en pratique chaque fois un nouveau jeu d'aléas.

3.1. Paire de clés selon la présente invention conférant une sécurité équivalente à la connaissance de la clé privée Q

La connaissance de deux triplets « en tenaille » équivaut à la connaissance de la clé privée Q .

Démonstration.

D'une part, le témoin se configure à partir des facteurs premiers p_1, p_2, p_3, \dots , de la clé privée Q et de l'exposant public de vérification v . Une fois configuré, le témoin peut produire une tenaille : il lui suffit d'utiliser deux fois le même jeu d'aléas.

D'autre part, deux triplets en tenaille se traduisent par les équations suivantes :

$$D \equiv r.Q^d \pmod{n} \text{ et } E \equiv r.Q^e \pmod{n} \quad \text{avec } 0 \leq d < e < v$$

$$\text{Par conséquent, } E/D \equiv Q^{e-d} \pmod{n}, \quad \text{avec } 0 < e-d < v$$

Voyons comment calculer la clé privée Q à partir du rapport E/D , lequel vaut $Q^{e-d} \pmod{n}$, c'est-à-dire l'une des $v-1$ valeurs $\{Q, Q^2, Q^3, \dots, Q^{v-1} \pmod{n}\}$, sachant que $Q^v \pmod{n}$ est la clé publique G ou son inverse modulo n .

La solution fait appel à l'identité de Bezout. Par définition, les coefficients de Bezout de v et de $e-d$ sont les deux entiers k et l vérifiant les relations

suivantes; l'algorithme de division d'Euclide permet de les calculer efficacement.

$$0 \leq k < e-d; \quad 0 \leq l < v; \quad k.v - l.(e-d) = \pm \text{pgcd}(e-d, v)$$

Dans le cas présent, v est premier et donc $\text{pgcd}(e-d, v) = 1$. Ce qui donne l'identité :

$$Q^{k.v-l.(e-d)} \equiv Q^{\pm 1} \pmod{n}$$

C'est-à-dire, $(Q^v)^k / (Q^{e-d})^l \equiv Q^{\pm 1} \pmod{n}$

- Lorsque $G \equiv Q^v \pmod{n}$ est utilisée, $G^k / (E/D)^l \pmod{n}$ vaut $Q \pmod{n}$ ou son inverse modulo n .

- Lorsque $G.Q^v \equiv 1 \pmod{n}$ est utilisée, $G^k . (E/D)^l \pmod{n}$ vaut $Q \pmod{n}$ ou son inverse modulo n .

3.2. Jeux de clés selon la présente invention conférant une sécurité équivalente à la connaissance de la factorisation de n

Les **nombre**s **GQ2** sont des produits de $l+1$ facteurs premiers distincts congrus à 3 (mod 4) avec la contrainte suivante : pour chacun de l petits nombres distincts, appelés **nombre**s de **base** et notés par ga, gb, \dots , ainsi que pour chacune de leurs combinaisons multiplicatives $ga.gb, \dots$, soit en tout $2^l - 1$ nombres représentés de façon générique par g , les deux équations $x^2 \equiv g \pmod{n}$ et $x^2 \equiv -g \pmod{n}$ n'ont pas de solution en x dans l'anneau des entiers modulo n . On dit alors que les nombres g et $-g$ sont deux résidus non quadratiques modulo n .

Note. « Petit » signifie plus petit que le plus petit des facteurs premiers. De préférence, les nombres de base sont les l premiers nombres premiers $ga = 2, gb = 3, \dots$

Les plus simples des nombres GQ2 sont les nombres de Williams avec un seul nombre de base $ga = 2$ et deux facteurs premiers, l'un congru à 3 (mod 8) et l'autre à 7 (mod 8).

Rappelons que pour chaque nombre g qui n'est pas un carré, chaque nombre premier congru à 3 (mod 4) et plus grand que g se classe dans l'une

des deux catégories suivantes :

- la catégorie où g est un résidu non quadratique (et donc $-g$ un résidu quadratique),
- la catégorie où $-g$ est un résidu non quadratique (et donc g un résidu quadratique).

Définition. Deux facteurs premiers sont **équivalents** ou **complémentaires** au regard d'un nombre g selon qu'ils appartiennent ou pas à la même catégorie au regard du nombre g .

Définition. Au regard de chaque nombre g , le **profil de j facteurs** est défini par une séquence de l bits en attribuant le symbole 1 au premier facteur ainsi que à tous les facteurs qui lui sont équivalents, c'est-à-dire qui ont le même symbole de Legendre, et le symbole 0 à tous les facteurs qui lui sont complémentaires, c'est-à-dire, qui ont l'autre symbole de Legendre.

Pour obtenir le profil au regard du produit de plusieurs nombres de base ga , gb , ..., on calcule le produit des symboles de Legendre, puis, on code le profil résultant en attribuant le symbole 1 au premier facteur ainsi que à tous les facteurs qui lui sont équivalents, c'est-à-dire, qui ont le même symbole de Legendre, et le symbole 0 à tous les facteurs complémentaires, c'est-à-dire, qui ont l'autre symbole de Legendre.

Pour pouvoir comparer des profils, il faut ranger les facteurs dans le même ordre, par exemple, dans l'ordre croissant.

3.2.1. Méthode systématique de construction des nombres GQ2

Voyons comment construire les nombres GQ2 de manière systématique, de façon à pouvoir intégrer simplement la méthode de construction dans un générateur de modules n .

Le premier facteur doit simplement être congru à 3 (mod 4). On notera toutefois son symbole de Legendre par rapport aux l nombres de base ga , gb , ...

Le deuxième facteur doit être complémentaire au regard du premier nombre

de base ga . Par exemple, lorsque $ga = 2$, un facteur doit être congru à 3 (mod 8) et l'autre à 7 (mod 8) : c'est un nombre de Williams. Par exemple encore, lorsque $ga = 3$, un facteur doit être congru à 1 (mod 3) et l'autre à 2 (mod 3), sachant qu'ils sont bien sûr tous deux congrus à 3 (mod 4). On notera également le symbole de Legendre du deuxième facteur par rapport aux l nombres de base ga, gb, \dots et on commencera à établir les $2^l - 1$ profils.

Le troisième facteur doit prendre en compte le deuxième nombre de base gb (par exemple, $gb = 3$ après $ga = 2$). Deux cas se présentent, selon que les deux premiers facteurs premiers sont équivalents ou complémentaires au regard du nombre gb .

- Lorsque les deux premiers facteurs premiers sont équivalents au regard du nombre gb , le nouveau facteur doit être complémentaire au regard du nombre gb .
- S'ils sont complémentaires, alors par rapport au premier facteur, le nouveau facteur doit être équivalent au regard de l'un des deux nombres ga ou gb et complémentaire au regard de l'autre.

On notera encore le symbole de Legendre du troisième facteur par rapport aux l nombres de base ga, gb, \dots et on commencera à établir les $2^l - 1$ profils. Ainsi, avec trois facteurs, pour les deux nombres de base, il y a trois profils possibles : 100, 110 et 101. La construction assure un profil différent pour chacun des trois nombres ga, gb et ga fois gb .

Le quatrième facteur doit prendre en compte le troisième nombre de base gc (par exemple, $gc = 5$ après $gb = 3$ et $ga = 2$). Deux cas se présentent, selon que les trois premiers facteurs sont équivalents ou pas au regard du nombre gc .

- Lorsque les trois premiers facteurs premiers sont équivalents au regard du nombre gc , le nouveau facteur doit être complémentaire au regard du nombre gc .

- S'ils ne sont pas équivalents, ils reproduisent le profil de l'un des trois nombres ga , gb ou ga fois gb (par exemple, 2, 3 ou 6), soit g ce nombre. Par rapport au premier facteur, le nouveau facteur doit être équivalent au regard de l'un des deux nombres g ou gc et complémentaire au regard de l'autre.

On notera encore le symbole de Legendre du quatrième facteur par rapport aux l nombres de base ga , gb , ... et on continuera à établir les $2^l - 1$ profils. Ainsi, avec quatre facteurs premiers, pour trois nombres de base, il y a sept profils possibles : 1000, 1100, 1010, 1001, 1110, 1101 et 1011. La construction assure un profil différent pour chacun des sept nombres suivants : les trois nombres de base : ga , gb , gc et leurs quatre combinaisons multiplicatives $ga.gb$, $ga.gc$, $gb.gc$ et $ga.gb.gc$.

Ensuite, la procédure se généralise aisément de la manière suivante.

Lorsque j facteurs sont déjà construits, le $j+1$ ième facteur doit prendre en compte un j ième nombre de base ; appelons g' ce nombre, par exemple, le j ième nombre premier après les $j-1$ premiers nombres premiers. Deux cas se présentent, selon que les j premiers facteurs sont équivalents ou pas au regard du nombre g' .

- Lorsque les j premiers facteurs premiers sont équivalents au regard du nombre g' , le nouveau facteur doit être complémentaire au regard du nombre g' .
- S'ils ne sont pas équivalents, ils reproduisent le profil de l'un des $j-1$ nombres ga , gb , ... ou de l'une de leurs combinaisons multiplicatives ga fois gb , ... ; appelons g ce nombre. Par rapport au premier facteur, le nouveau facteur doit être équivalent au regard de l'un des deux nombres g ou g' et complémentaire au regard de l'autre.

On notera encore le symbole de Legendre du $j+1$ ième facteur par rapport aux l nombres de base ga , gb , ... et on continuera à établir les $2^l - 1$ profils.

3.2.2. Utilisation cryptographique des nombres GQ2

Voici deux motifs d'intérêt cryptographique pour les nombres GQ2.

- Produire des paires de clés pour des schémas de signature numérique qui étendent l'usage de l'exposant 2 à des modules n ayant plus de deux facteurs premiers.
- Produire des jeux de clés pour des schémas GQ2 d'authentification dynamique ou de signature numérique.

3.2.2.1 Dans l'annexe A de ISO/CEI 9796, extension de l'usage des exposants pairs à des modules ayant plus de deux facteurs premiers, chaque facteur étant congru à 3 (mod 4).

⇒ Pour éviter de divulguer la factorisation du module n en appliquant la fonction privée de signature à un argument, c'est-à-dire, en calculant une racine carrée (mod n), il faut égaliser les symboles de Legendre de l'argument par rapport à l'ensemble des facteurs premiers du module n . Cette égalisation se fait en divisant par un « égaliseur » approprié. A la vérification, il faut décoder le résultat, c'est-à-dire, déduire la valeur de l'égaliseur mis en œuvre à la signature.

Il faut d'abord choisir et normaliser un ou plusieurs petits nombres. Ces nombres sont de préférence les l premiers nombres premiers. Nous les nommerons les **égaliseurs de base** et les noterons par $ga, gb \dots$. Les l égaliseurs de base complétés par leurs combinaisons multiplicatives, soit $2^l - 1$ nombres en tout, constituent l'ensemble des **égaliseurs**. Voyons comment utiliser les égaliseurs.

- Deux facteurs — On choisit d'abord un égaliseur de base ga (par exemple, $ga = 2$; on pourrait aussi bien prendre 3, 5 ou 7 ...). Puis, on choisit deux facteurs premiers complémentaires au regard de l'égaliseur ga (par exemple, lorsque $ga = 2$, un facteur est congru à 3 (mod 8) et l'autre à 7 (mod 8)). Lorsqu'un argument est soumis à la fonction privée

de signature, on calcule le symbole de Jacobi de l'argument par rapport au module n . S'il vaut $+1$, on garde l'argument tel quel. S'il vaut -1 , on remplace l'argument par l'argument divisé par l'égaliseur ga pour mettre le symbole de Jacobi à $+1$; suite à cette opération, le symbole de Jacobi de l'argument vaut $+1$, c'est-à-dire que les symboles de Legendre de l'argument sont alors tous les deux égaux à -1 ou bien tous les deux égaux à $+1$. Cette méthode figure dans l'annexe A de la norme ISO/CEI 9796.

- Trois facteurs — On choisit d'abord deux égaliseurs de base, par exemple, $ga = 2$ et $gb = 3$. Puis, on choisit les trois facteurs premiers de sorte que $ga = 2$, $gb = 3$ et $ga.gb = 6$ soient tous les trois des résidus non quadratiques (mod n). Lorsque les trois symboles de Legendre de l'argument sont inégaux, on les égalise en divisant l'argument selon le cas par $ga = 2$, $gb = 3$ ou $ga.gb = 6$, c'est-à-dire, par l'égaliseur qui présente le même profil que l'argument.
- Quatre facteurs — On choisit d'abord trois égaliseurs de base, par exemple, $ga = 2$, $gb = 3$ et $gc = 5$. Puis, on choisit les quatre facteurs premiers de sorte que les sept nombres 2, 3, 5, 6, 10, 15 et 30 soient des résidus non quadratiques (mod n). Lorsque les quatre symboles de Legendre de l'argument sont inégaux, on les égalise en divisant l'argument par l'égaliseur approprié : 2, 3, 5, 6, 10, 15 ou 30, c'est-à-dire, celui qui présente le même profil que l'argument.
- Cinq facteurs — On choisit d'abord quatre égaliseurs de base, par exemple, $ga = 2$, $gb = 3$, $gc = 5$ et $gd = 7$. Puis, on choisit les cinq facteurs premiers de sorte que les quinze nombres 2, 3, 5, 6, 7, 10, 14, 15, 21, 30, 35, 42, 70, 105, 210 soient des résidus non quadratiques (mod n). Lorsque les symboles de l'argument sont inégaux, on les égalise en divisant l'argument par l'égaliseur approprié : 2, 3, 5, 6, 7, 10, 14, 15, 21, 30, 35, 42, 70, 105, 210, c'est-à-dire celui qui a le même

profil que l'argument.

- Et ainsi de suite.

3.2.2.2. GQ2 - Le module est le produit de facteurs premiers congrus à 3 (mod 4).

5 \Rightarrow La propriété à assurer est que toute paire de triplets GQ2 en tenaille révèle une factorisation non triviale du module.

Il faut d'abord choisir un ou plusieurs petits nombres. Ce sont de préférence les l premiers nombres premiers. Nous les appellerons les **racines triviales de base** et les noterons par $ga, gb, gc \dots$. Les l racines triviales de base
10 complétées par leurs combinaisons multiplicatives, soit, en tout, $2^l - 1$ nombres, constituent l'ensemble des **racines triviales**.

- Deux facteurs — Il faut d'abord sélectionner une seule racine triviale de base ga (par exemple, $ga = 2$; on pourrait aussi bien prendre 3, 5 ou 7 ...). Il faut ensuite choisir les deux facteurs de sorte que la racine triviale
15 ga soit un résidu non quadratique (mod n), c'est-à-dire que les facteurs soient « complémentaires » au regard de la racine triviale ga .
- Trois facteurs — Il faut d'abord sélectionner deux racines triviales de base, par exemple, $ga = 2$ et $gb = 3$. Il faut ensuite choisir les trois facteurs de sorte que les trois (2 puissance 2 moins 1) racines triviales
20 ga, gb et $ga.gb$, par exemple, 2, 3 et 6, soient des résidus non quadratiques (mod n).
- Quatre facteurs — Il faut d'abord sélectionner trois racines triviales de base, par exemple, $ga = 2, gb = 3$ et $gc = 5$. Il faut choisir ensuite les quatre facteurs premiers de sorte que les nombres 2, 3 et 5, ainsi que
25 leurs combinaisons multiplicatives, c'est-à-dire, 6, 10, 15 et 30, soient tous les sept (2 puissance 3 moins 1) des résidus non quadratiques (mod n). Ces sept nombres sont les racines triviales.
- Cinq facteurs — Il faut d'abord sélectionner quatre racines triviales de base, par exemple, $ga = 2, gb = 3, gc = 5$ et $gd = 7$. Il faut choisir

ensuite les cinq facteurs premiers de sorte que les nombres 2, 3, 5 et 7, ainsi que leurs combinaisons multiplicatives, c'est-à-dire, 6, 10, 14, 15, 21, 30, 35, 42, 70, 105 et 210, soient tous les quinze (2^4 puissance 4 moins 1) des résidus non quadratiques (mod n). Ces quinze nombres sont les racines triviales.

- Et ainsi de suite.

Dans les mécanismes GQ2 d'authentification dynamique et de signature numérique, toute paire de triplets GQ2 en tenaille révèle une des k valeurs $\{Q, Q^2, Q^4, \dots$ jusqu'au $k-1$ ième carré de Q (mod $n\}$ où Q est une des 2^{l-1} combinaisons multiplicatives des l clés privées de base QA, QB, \dots Ceci revient à connaître le $k-1$ ième carré d'un nombre Q (mod n) ; ce nombre ou son inverse (mod n) est une racine carrée (mod n) de la combinaison correspondante des clés publiques, combinaison que nous notons par $G = g^2$. Nommons q ce nombre.

La mise en œuvre de nombres GQ2, c'est-à-dire, de modules n construits selon la méthode précédentes à partir de $l+1$ facteurs premiers et de l racines de base $ga\ gb\ \dots$, assurent que, pour toute paire de triplets en tenaille, le nombre q obtenu ci-dessus est une racine carrée non triviale de $G = g^2$ dans l'anneau des entiers modulo n . Le module n divise $q^2 - g^2$, alors qu'il ne divise ni $q-g$ ni $q+g$. Ainsi, avec des nombres GQ2, toute paire de triplets GQ2 en tenaille révèle une factorisation non triviale du module n . Sur l'ensemble des paires de triplets en tenaille, toutes les factorisations non triviales sont possibles : la factorisation est déterminée par le profil du nombre g concerné : d'une côté, tous les facteurs premiers équivalents au premier facteur premier, de l'autre tous les autres facteurs premiers, c'est-à-dire, ceux qui sont complémentaires au premier facteur premier.

4. Sécurité du nouveau procédé

D'une manière générale, la sécurité des protocoles « sans transfert de connaissance » s'analyse selon trois notions de base définies dans l'article de base de Shafi Goldwasser, Silvio Micali et Charles Rackoff.

5 Dans le cas qui nous intéresse, une entité proclame : « — *Voici un module n , un exposant de vérification v et une clé publique G ; j'utilise la factorisation de n et je connais la clé privée Q .* »

Par définition, lorsque l'entité connaît les facteurs premiers, c'est un témoin. A chaque appel, le témoin produit de manière privée un triplet que
10 le contrôleur accepte. Par conséquent, la procédure est complète.

Par définition, lorsque l'entité ne connaît pas les facteurs premiers, c'est un tricheur. A chaque appel, le tricheur a une chance sur v de deviner le défi d (si les v défis sont équiprobables) ; il peut donc anticiper un défi, n'importe lequel, et ainsi tromper le contrôleur ; s'il pouvait anticiper un deuxième
15 défi après avoir produit l'engagement, il connaîtrait une paire de triplets en tenaille, ce qui contredit la définition du tricheur. Par conséquent, la procédure est robuste.

Note. La présente version fait fi du symbole de Jacobi ; le prix à payer est la perte d'un bit de défi par paire de clés selon la présente invention. Le
20 procédé ne marche pas pour $k = 1$; le tricheur a une stratégie gagnante totale. A partir de $k = 2$, le tricheur n'a plus qu'une stratégie gagnante partielle : il peut anticiper deux défis mais pas trois.

Quelle que soit la manière dont se comporte le monde extérieur, il reçoit seulement l'information que le témoin connaît les facteurs premiers. Plus
25 précisément, quelle que soit l'information émise par le témoin, n'importe qui aurait pu la constituer sans interaction avec le témoin ; n'importe qui peut simuler les transmissions et produire un enregistrement qui reproduit les caractéristiques statistiques des informations recueillies lors d'une interaction avec le témoin. Durant l'interaction, un observateur ne peut pas

distinguer un honnête témoin d'un faux témoin utilisant une liste de défis convenue à l'avance. Après l'interaction, un juge ne peut pas distinguer les deux types d'enregistrements. En effet, on ne peut pas distinguer un enregistrement de triplets produits de manière publique et un enregistrement de triplets produits de manière privée. Par conséquent, la procédure utilisée par le témoin ne laisse filtrer aucune information sur la valeur des facteurs premiers.

L'entité qui prouve pilote toujours le même témoin fonctionnant toujours de la même manière : le témoin utilise les facteurs premiers et la clé privée Q sans les révéler ; le témoin assure la protection des facteurs premiers et de la clé privée Q . Le contrôleur vérifie la clé privée Q sans en prendre connaissance. La procédure se déroule « sans transfert de connaissance ». Certaines paires de clés selon la présente invention sont telles que la connaissance de la clé privée Q implique la connaissance de la factorisation du module n . Avec le nouveau procédé, la factorisation et la clé privée Q ne s'usent pas, même quand on s'en sert.

5. Performances du nouveau procédé avec $\nu = 2^t$

Dans cette évaluation, on fait l'hypothèse que la valeur de G est petite, par exemple, $G = 4$. La charge de travail du témoin et la charge de travail du contrôleur dépendent du niveau de sécurité recherché, c'est-à-dire du produit de deux nombres : le nombre j de triplets produits à chaque appel au témoin et la valeur donnée au paramètre de sécurité k moins un (en effet, on perd un bit de défi en laissant tomber le symbole de Jacobi).

Pour une authentification avec $j \cdot (k-1) = 16$ avec $j = 1$,

le témoin doit effectuer 17 carrés pour calculer l'engagement R , puis, en moyenne 16 carrés et 8 multiplications plus une multiplication pour calculer la réponse D , soit 41 opérations (mod n) ;

cette charge est divisée par deux avec deux facteurs premiers, soit 20 opérations (mod n) ;

cette charge est divisée par trois avec trois facteurs premiers, soit environ 14 opérations (mod n) ;

et ainsi de suite.

le contrôleur doit effectuer 17 carrés (mod n).

5 Pour une signature avec $j.(k-1) = 80$ avec $j = 1$,

le témoin doit effectuer 81 carrés pour calculer l'engagement R , puis, en moyenne 80 carrés et 40 multiplications plus une multiplication pour calculer la réponse D , soit 202 opérations (mod n) ;

10 cette charge est divisée par deux avec deux facteurs premiers, soit 100 opérations (mod n) ;

cette charge est divisée par trois avec trois facteurs premiers, soit 67 opérations (mod n) ;

et ainsi de suite.

le contrôleur doit effectuer 81 carrés (mod n).

15 **Remarque.** Pour une valeur donnée du niveau de sécurité $j.k$, le choix $j = 1$ ne change pratiquement pas la charge de travail du témoin, ni celle du contrôleur ; elle minimise toutefois le nombre de triplets produits, c'est-à-dire, la charge de transmission pour mener à bien l'opération, que cette opération soit une authentification ou une signature.

20 Utilisons plusieurs paires de clés selon la présente invention, toutes avec le même exposant public de vérification v . Cela fait apparaître un niveau de sécurité $j.(k-1).l$ où l est le nombre de paires de clés selon la présente invention. Le fait d'utiliser plusieurs paires de clés selon la présente invention diminue la charge de travail du témoin, ainsi que la charge de travail du contrôleur.

25 Dans le tableau ci-dessous, M représente une multiplication (mod n) et X un carré (mod n). Rappelons que sur le composant ST 16601 pour carte à puce, avec une horloge normalisée à 3,579545 MHz, le carré modulo pour 512 bits se fait en 150 ms et la multiplication modulo en 200 ms.

$(k-1).l = 16$	$l = 1$	$l = 2$	$l = 4$	$l = 8$	$l = 16$
Engagement	17 X	9 X	5 X	3 X	2 X
Réponse	1 M + 16 X + 8 M	1 M + 8 X + 8 X	1M + 4X+ 8M	1 M + 2 X + 8 M	1 M + 1 X + 8 M
Total du témoin	33 X + 9 M	17 X + 9 M	9 X + 9 M	5 X + 9 M	3 X + 9 M
Trois facteurs	11 X + 3 M	6 X + 3 M	3 X + 3 M	2 X + 3 M	1 X + 3 M
Vérification	17 X	9 X	5 X	3 X	2 X

Le compromis pour $l = 4$ est très attrayant parce que, compte tenu des restes chinois avec un module à trois facteurs premiers, le terminal et la carte ont à peu près la même charge de travail. Il est préconisé d'utiliser les clés publiques $GA = 4$, $GB = 9$, $GC = 25$, $GD = 49$.

Revendications

1. Procédé pour diminuer la charge de travail pendant une session destinée à prouver à un contrôleur,

- l'authenticité d'une entité et/ou

5 - l'origine et l'intégrité d'un message m ,

ledit procédé met en œuvre trois entités :

- une première entité appelée témoin dispose des facteurs premiers

$p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$,

10 ledit témoin dispose aussi

* des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ..., représentant des clés privées QA, QB, \dots

* des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

15 * des exposants publics de vérification vx, vy, \dots

lesdites clés privées et clés publiques étant liées par des relations du type :

$$GA \cdot QA^x \bmod n \equiv 1 \text{ ou } GA \equiv QA^x \bmod n$$

lesdits exposants publics de vérification vx, vy, \dots étant utilisés par le témoin pour calculer des engagements R en effectuant des opérations du type :

$$R_i \equiv r_i^x \bmod p_i$$

où r_i est un entier, associé au nombre premier p_i , tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, r_3, \dots\}$,

le témoin tire au hasard une ou plusieurs collections d'aléas de telle sorte que, pour chaque exposant public de vérification v , il y a autant d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$,

25

- une deuxième entité pilote dudit témoin

* appelée démonstrateur dans le cas de la preuve de l'authenticité d'une entité ou de l'authenticité d'un message,

* appelée signataire dans les cas de la preuve de l'origine et de l'intégrité d'un message,

- une troisième entité appelée contrôleur vérifie l'authentification ou l'origine et l'intégrité d'un message,

5 ledit témoin reçoit de la deuxième entité ou du contrôleur un ou plusieurs défis d tel que $0 \leq d \leq vx - 1$ et calcule à partir de ce défi une ou plusieurs réponses D en effectuant des opérations du type :

$$D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \bmod p_i$$

où r_i est un aléa tel que $0 < r_i < p_i$

10 de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacune des réponses D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

ledit contrôleur recevant une ou plusieurs réponses D calcule à partir desdites réponses des engagements R' en effectuant des opérations du type :

$$R' \equiv GA^{dA} \cdot GB^{dB} \cdot \dots D' \bmod n$$

ou du type :

$$R' \cdot GA^{dA} \cdot GB^{dB} \cdot \dots \equiv D' \bmod n$$

ledit contrôleur vérifie que les triplets $\{R', d, D\}$ sont cohérents.

20 2. Procédé pour diminuer la charge de travail pendant une session destinée à prouver à un contrôleur,

- l'authenticité d'une entité et/ou
- l'origine et l'intégrité d'un message m ,

ledit procédé met en œuvre trois entités :

25 - une première entité appelée témoin dispose des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$,

ledit témoin dispose aussi

- * des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i,$

...), ..., représentant des clés privées QA, QB, \dots

* des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

* d'un exposant public de vérification v

5 lesdites paires de clés privées et publiques étant liées par des relations du type :

$$GA \cdot QA' \bmod n \equiv 1 \text{ ou } GA \equiv QA' \bmod n$$

ledit exposant public de vérification v étant utilisé par le témoin pour calculer des engagements R ,

10 • en effectuant des opérations du type :

$$R_i \equiv r_i' \bmod p_i$$

où r_i est un entier, tiré au hasard, associé au nombre premier p_i , tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, r_3, \dots\}$,

• puis en appliquant la méthode des restes chinois,

15 le témoin tire au hasard une ou plusieurs collections d'aléas de telle sorte qu'il y a autant d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$, de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

20 - une deuxième entité pilote dudit témoin,

* appelée démonstrateur dans le cas de la preuve de l'authenticité d'une entité ou de l'authenticité d'un message,

* appelée signataire dans les cas de la preuve de l'origine et de l'intégrité d'un message,

25 - une troisième entité appelée contrôleur vérifie l'authentification ou l'origine et l'intégrité d'un message,

ledit témoin reçoit de la deuxième entité ou du contrôleur, des collections de défis d $\{dA, dB, \dots\}$ tels que $0 \leq dA \leq v - 1$, le nombre des collections de défis d étant égal au nombre d'engagements R , chaque collection $\{dA,$

$dB, \dots\}$ comprenant un nombre de défis égal au nombre de paires de clés, ledit témoin calcule à partir de chacune desdites collections de défis $\{dA, dB, \dots\}$ des réponses D

- en effectuant des opérations du type :

$$5 \quad D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \bmod p_i$$

- puis en appliquant la méthode des restes chinois,

de telle sorte qu'il y a autant de réponses D que d'engagements R et de défis d ,

10 de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n

ledit contrôleur recevant une réponse D calcule à partir de cette réponse un engagement R' en effectuant des opérations du type :

$$R' \equiv GA^{dA} \cdot GB^{dB} \cdot \dots D' \bmod n$$

15 ou du type :

$$R' \cdot GA^{dA} \cdot GB^{dB} \cdot \dots \equiv D' \bmod n$$

ledit contrôleur vérifie que les triplets $\{R', d, D\}$ sont cohérents.

3. Procédé selon la revendication 2 pour diminuer la charge de travail pendant une session destinée à prouver à un contrôleur l'authenticité d'une entité ;

20 ledit procédé met en œuvre trois entités :

1 - une première entité appelée témoin dispose des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$,

25 ledit témoin dispose aussi

* des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ..., représentant des clés privées QA, QB, \dots

* des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

* d'un exposant public de vérification v
 lesdites paires de clés privées et publiques étant liées par des relations du type :

$$GA.QA' \bmod n \equiv 1 \text{ ou } GA \equiv QA' \bmod n$$

5

2 - une deuxième entité pilote dudit témoin appelée démonstrateur

3 - une troisième entité appelée contrôleur vérifie l'authentification, pour prouver l'authenticité d'une entité, ledit témoin, ledit démonstrateur et ledit contrôleur exécutent les étapes suivantes :

• **étape 1. engagement R du témoin :**

10

- à chaque appel, le témoin tire au hasard et en privé au moins une collection de nombres entiers $\{r_1, r_2, r_3, \dots\}$, telle que, pour chaque facteur premier p_i , chaque collection comporte un aléa r_i positif et plus petit que p_i ,
 - pour chaque facteur premier p_i , le témoin élève chaque aléa r_i à la puissance v ième modulo p_i

15

$$R_i \equiv r_i^v \bmod p_i$$

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

20

- puis, le témoin établit chaque engagement R modulo n selon la méthode des restes chinois,
 de telle sorte qu'il y a autant d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$,

• **étape 2. défi d destiné au témoin :**

25

- le démonstrateur transmet tout ou partie de chaque engagement R au contrôleur,
 - le contrôleur, après avoir reçu tout ou partie de chaque engagement R , produit au moins une collection de défis d $\{dA, dB, \dots\}$ tels que $0 \leq dA \leq v - 1$, le nombre des collections de défis d étant égal au nombre d'engagements R , chaque collection $\{dA, dB, \dots\}$ comprenant un nombre

de défis égal au nombre de paires de clés,

• **étape 3. réponse du témoin au défi d :**

- ledit témoin calcule des réponses **D** à partir desdites collections de défis **d** {dA, dB, ...} reçues du contrôleur

5 en effectuant des opérations du type :

$$D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \bmod p_i$$

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

10 puis en appliquant la méthode des restes chinois,

de telle sorte qu'il y a autant de réponses **D** calculées par le témoin que d'engagements **R** et de défis **d**,

• **étape 4. données destinées au contrôleur :**

- le démonstrateur transmet au contrôleur chaque réponse **D**,

15 • **étape 5. vérification par le contrôleur :**

ledit contrôleur calcule à partir de chaque réponse **D** un engagement **R'** en effectuant des opérations du type :

$$R' \equiv GA^{dA} \cdot GB^{dB} \cdot \dots D' \bmod n$$

ou du type :

20
$$R' \cdot GA^{dA} \cdot GB^{dB} \cdot \dots \equiv D' \bmod n$$

ledit contrôleur vérifie que chaque engagement reconstruit **R'** reproduit tout ou partie de chaque engagement **R** transmis à l'étape 2 par le démonstrateur.

25 4. Procédé selon la revendication 2 pour diminuer la charge de travail pendant une session destinée à prouver à un contrôleur l'authenticité d'un message **m**,

ledit procédé met en œuvre trois entités :

1 - une première entité appelée témoin dispose des facteurs premiers $P_1, P_2, \dots (P_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public **n** tel

que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$,

ledit témoin dispose aussi

* des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ..., représentant des clés privées QA, QB, \dots

5 * des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

* d'un exposant public de vérification v

lesdites paires de clés privées et publiques étant liées par des relations du type :

10 $GA \cdot QA' \bmod n \equiv 1$ ou $GA \equiv QA' \bmod n$

2 - une deuxième entité pilote dudit témoin appelée démonstrateur,

3 - une troisième entité appelée contrôleur vérifie l'authentification, pour prouver l'authenticité d'un message ledit témoin, ledit démonstrateur et ledit contrôleur exécutent les étapes suivantes :

15 • étape 1. engagement R du témoin :

- à chaque appel, le témoin tire au hasard et en privé au moins une collection de nombres entiers $\{r_1, r_2, r_3, \dots\}$, telle que pour chaque facteur premier p_i , chaque collection comporte un aléa r_i positif et plus petit que p_i ,

20 - pour chaque facteur premier p_i , le témoin élève chaque aléa r_i à la puissance v ième modulo p_i

$$R_i \equiv r_i^v \bmod p_i$$

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

25 - puis, le témoin établit chaque engagement R modulo n selon la méthode des restes chinois,

de telle sorte qu'il y a autant d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$,

• étape 2. défi d destiné au témoin :

- le démonstrateur applique une fonction de hachage f ayant comme arguments le message m et chaque engagement R pour un jeton T ,
- le démonstrateur transmet le jeton T au contrôleur,
- le contrôleur, après avoir reçu le jeton T , produit au moins une collection de défis d $\{dA, dB, \dots\}$ tels que $0 \leq dA \leq v - 1$, le nombre des collections de défis d étant égal au nombre d'engagements R , chaque collection $\{dA, dB, \dots\}$ comprenant un nombre de défis égal au nombre de paires de clés,

• **étape 3. réponse du témoin au défi d :**

- ledit témoin calcule des réponses D à partir desdites collections de défis d $\{dA, dB, \dots\}$ reçues du contrôleur en effectuant des opérations du type :

$$D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \bmod p_i$$

puis en appliquant la méthode des restes chinois,

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n , de telle sorte qu'il y a autant de réponses D calculées par le témoin que d'engagements R et de défis d ,

• **étape 4. données destinées au contrôleur :**

- le démonstrateur transmet au contrôleur chaque réponse D ,

• **étape 5. vérification par le contrôleur :**

ledit contrôleur calcule à partir de chaque réponse D un engagement R' en effectuant des opérations du type :

$$R' \equiv GA^{dA} \cdot GB^{dB} \cdot \dots D' \bmod n$$

ou du type :

$$R' \cdot GA^{dA} \cdot GB^{dB} \cdot \dots \equiv D' \bmod n$$

ledit contrôleur applique la fonction de hachage f ayant comme arguments le message m et chaque engagement reconstruit R' pour reconstruire le jeton T' ,

ledit contrôleur vérifie que le jeton T' est identique au jeton T transmis à l'étape 2 par le démonstrateur.

5 5. Procédé selon la revendication 2 pour diminuer la charge de travail pendant une session destinée à prouver à un contrôleur la signature numérique d'un message m ,

ledit procédé met en œuvre trois entités :

1 - une première entité appelée témoin dispose des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$,

10 ledit témoin dispose aussi

* des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ..., représentant des clés privées QA, QB, \dots

* des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

15 * d'un exposant public de vérification v

lesdites paires de clés privées et publiques étant liées par des relations du type :

$$GA \cdot QA^v \bmod n \equiv 1 \text{ ou } GA \equiv QA^v \bmod n$$

2 - une deuxième entité pilote dudit témoin appelée signataire,

20 3 - une troisième entité appelée contrôleur vérifie l'authentification, pour prouver la signature d'un message ledit témoin, ledit démonstrateur et ledit contrôleur exécutent les étapes suivantes :

• **étape 1. engagement R du témoin :**

25 - à chaque appel, le témoin tire au hasard et en privé au moins une collection de nombres entiers $\{r_1, r_2, r_3, \dots\}$, telle que, pour chaque facteur premier p_i , chaque collection comporte un aléa r_i positif et plus petit que p_i ,
 - pour chaque facteur premier p_i , le témoin élève chaque aléa r_i à la puissance v ième modulo p_i

$$R_i \equiv r_i^v \bmod p_i$$

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

- puis, le témoin établit chaque engagement R modulo n selon la méthode des restes chinois,

de telle sorte qu'il y a autant d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$,

• **étape 2. défi d destiné au témoin :**

- le signataire applique une fonction de hachage f ayant comme arguments le message m et chaque engagement R pour obtenir au moins une collection de défis d $\{dA, dB, \dots\}$ tels que $0 \leq dA \leq v - 1$, le nombre des collections de défis d étant égal au nombre d'engagements R , chaque collection $\{dA, dB, \dots\}$ comprenant un nombre de défis égal au nombre de paires de clés,

- le signataire transmet les collections de défis d au témoin,

• **étape 3. réponse du témoin au défi d :**

- ledit témoin calcule des réponses D à partir desdites collections de défis d $\{dA, dB, \dots\}$ reçues du contrôleur

en effectuant des opérations du type :

$$D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \bmod p_i$$

puis en appliquant la méthode des restes chinois,

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

de telle sorte qu'il y a autant de réponses D calculées par le témoin que d'engagements R et de défis d ,

- ledit témoin transmet les réponses D au signataire et/ou au contrôleur,

• **étape 4. données destinées au contrôleur :**

- le signataire transmet un message signé au contrôleur comprenant :

/ le message **m**,

/ les collections de défis **d** ou les engagements **R**,

/ chaque réponse **D**

• **étape 5. vérification par le contrôleur :**

5 **cas où le contrôleur reçoit la collection des défis d**,
dans le cas où le contrôleur reçoit la collection des défis **d** et des réponses **D**, ledit contrôleur calcule à partir de chaque réponse **D** un engagement **R'** en effectuant des opérations du type :

$$R' \equiv GA^{d^A} \cdot GB^{d^B} \cdot \dots D' \text{ mod } n$$

10 ou du type :

$$R' \cdot GA^{d^A} \cdot GB^{d^B} \cdot \dots \equiv D' \text{ mod } n$$

ledit contrôleur applique la fonction de hachage **f** ayant comme arguments le message **m** et chaque engagement reconstruit **R'** pour reconstruire chaque défi **d'**,

15 ledit contrôleur vérifie que chaque défi **d'** reconstruit est identique au défi **d** figurant dans le message signé,

cas où le contrôleur reçoit la collection des engagements R

dans le cas où le contrôleur reçoit la collection des engagements **R** et des réponses **D**, ledit contrôleur applique la fonction de hachage **f** ayant comme arguments le message **m** et chaque engagement **R** pour reconstruire chaque défi **d'**,

20 ledit contrôleur reconstruit alors la collection des engagements **R'** en effectuant des opération du type

$$R' \equiv GA^{d^A} \cdot GB^{d^B} \cdot \dots D' \text{ mod } n$$

25 ou du type :

$$R' \cdot GA^{d^A} \cdot GB^{d^B} \cdot \dots \equiv D' \text{ mod } n$$

ledit contrôleur vérifie que chaque engagement **R'** reconstruit est identique à l'engagement **R** figurant dans le message signé,

6. Procédé selon l'une quelconque des revendications 1 à 5 tel que

les composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ... des clés privées QA, QB, \dots sont des nombres tirés au hasard à raison d'une composante QA_i, QB_i, \dots pour chacun desdits facteurs premiers p_i , lesdites clés privées QA, QB , pouvant être calculées à partir desdites composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ... par la méthode des restes chinois,

lesdites clés publiques GA, GB, \dots étant calculée

- en effectuant des opérations du type :

$$GA_i \equiv QA_i' \bmod p_i$$

- puis en appliquant la méthode des restes chinois pour établir GA tel que

$$GA \equiv QA' \bmod n$$

ou bien tel que

$$GA.QA' \bmod n \equiv 1$$

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des GA_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n .

7. Procédé selon la revendication 6 tel que l'exposant public de vérification v est un nombre premier,

de sorte que la paire de clés GA, QA confère une sécurité équivalente à la connaissance de la clé privée QA .

8. Procédé selon l'une quelconque des revendications 1 à 5 tel que l'exposant public de vérification v est du type

$$v = a^k$$

ou k est un paramètre de sécurité plus grand que 1.

9. Procédé selon la revendication 8 tel que :

- l'exposant public de vérification v est du type

$$v = 2^k$$

ou k est un paramètre de sécurité plus grand que 1,

- la clé publique GA est un carré gA^2 inférieur à n choisi de telle

sorte que les deux équations

$$x^2 \equiv gA \bmod n \quad \text{et} \quad x^2 \equiv -gA \bmod n$$

n'ont pas de solution en x dans l'anneau des entiers modulo n ,

- lesdites composantes $QA_1, QA_2, \dots (QA_i, \dots)$ de la clé privée QA

sont telles que :

$$GA \equiv QA_i^{2 \exp(k)} \bmod p_i$$

ou bien telles que :

$$GA \cdot QA_i^{2 \exp(k)} \bmod p_i \equiv 1$$

on les obtient en extrayant la k ième racine carrée de GA dans le corps de Galois $CG(p_i)$

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer pour calculer chacun des QA_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

de sorte que la paire de clés GA, QA confère une sécurité équivalente à la connaissance de la factorisation de n .

10. Procédé selon la revendication 9 tel que pour extraire la k ième racine carrée de GA dans le corps de Galois $CG(p_i)$,

* dans le cas où le facteur premier p_i est congru à 3 modulo 4, on applique notamment un algorithme du type :

$$x = (p+1)/4 ; y \equiv x^k \bmod (p-1) ; z = y ; QA_i \equiv GA^z \bmod p_i$$

* dans le cas où le facteur premier p_i est congru à 1 modulo 4, on utilise les suites de Lucas.

11. Système pour diminuer la charge de travail pendant une session destinée à prouver à un serveur contrôleur,

- l'authenticité d'une entité et/ou
- l'origine et l'intégrité d'un message m ,

ledit procédé met en œuvre trois entités :

- une première entité, appelée dispositif témoin, contenue notamment dans un objet nomade se présentant par exemple sous la forme d'une carte

bancaire à microprocesseur,

le dispositif témoin dispose d'une première zone mémoire contenant des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$,

5 ledit dispositif témoin dispose aussi d'une deuxième zone mémoire contenant :

* des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ..., représentant des clés privées QA, QB, \dots

10 * des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

* des exposants publics de vérification vx, vy, \dots

lesdites clés privées et clés publiques étant liées par des relations du type :

$$GA \cdot QA^x \bmod n \equiv 1 \text{ ou } GA \equiv QA^x \bmod n$$

15 ledit dispositif témoin comporte aussi des premiers moyens de calcul pour calculer des engagements R en effectuant des opérations du type :

$$R_i \equiv r_i^x \bmod p_i$$

où r_i est un aléa tel que $0 < r_i < p_i$,

20 de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer par lesdits premiers moyens de calcul pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

- une deuxième entité appelée dispositif pilote dudit dispositif témoin pouvant être également contenue notamment dans ledit objet nomade,

25 ledit dispositif pilote est appelé

* dispositif démonstrateur dans le cas de la preuve de l'authenticité d'une entité ou de l'authenticité d'un message,

* dispositif de signature dans les cas de la preuve de l'origine et de l'intégrité d'un message,

- une troisième entité appelée dispositif contrôleur se présentant notamment sous la forme d'un terminal et/ou d'un serveur distant connecté à un réseau de communication informatique,

ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique audit dispositif témoin,

ledit dispositif contrôleur vérifie l'authentification ou l'origine et l'intégrité d'un message,

ledit dispositif témoin reçoit du dispositif pilote ou du dispositif contrôleur un ou plusieurs défis d tel que $0 \leq d \leq vx - 1$ et comporte des deuxièmes moyens de calcul pour calculer à partir dudit défi d une ou plusieurs réponses D en effectuant des opérations du type :

$$D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \bmod p_i$$

où r_i est un entier, associé au nombre premier p_i , tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, r_3, \dots\}$,

le témoin tire au hasard une ou plusieurs collections d'aléas de telle sorte que, pour chaque exposant public de vérification v , il y a autant d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$,

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer par lesdits deuxièmes moyens de calcul pour calculer chacune des réponses D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

ledit dispositif contrôleur, recevant une ou plusieurs réponses D , comporte des troisièmes moyens de calcul pour calculer à partir desdites réponses D des engagements R' en effectuant des opérations du type :

$$R' \equiv GA^{dA} \cdot GB^{dB} \cdot \dots D' \bmod n$$

ou du type :

$$R' \cdot GA^{dA} \cdot GB^{dB} \cdot \dots \equiv D' \bmod n$$

ledit dispositif contrôleur comporte des quatrièmes moyens de calcul pour

vérifier que les triplets $\{R', d, D\}$ sont cohérents.

12. Système pour diminuer la charge de travail pendant une session destinée à prouver à un contrôleur,

- l'authenticité d'une entité et/ou
- l'origine et l'intégrité d'un message m ,

ledit procédé met en œuvre trois entités :

- une première entité appelée dispositif témoin, contenue notamment dans un objet nomade se présentant par exemple sous la forme d'une carte bancaire à microprocesseur,

ledit dispositif témoin dispose d'une première zone mémoire contenant des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$,

ledit dispositif témoin dispose aussi d'une deuxième zone mémoire contenant

- * des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ..., représentant des clés privées QA, QB, \dots

- * des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

- * un exposant public de vérification v

lesdites paires de clés privées et publiques étant liées par des relations du type :

$$GA \cdot QA^v \bmod n \equiv 1 \text{ ou } GA \equiv QA^v \bmod n$$

ledit dispositif témoin comporte aussi des premiers moyens de calcul pour calculer des engagements R ,

- en effectuant des opérations du type :

$$R_i \equiv r_i^v \bmod p_i$$

où r_i est un entier, tiré au hasard, associé au nombre premier p_i , tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, r_3, \dots\}$,

- puis en appliquant la méthode des restes chinois,

le témoin tire au hasard une ou plusieurs collections d'aléas de telle sorte qu'il y a autant d'engagements \mathbf{R} que de collections d'aléas $\{\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \dots\}$, de sorte que le nombre d'opérations arithmétiques modulo \mathbf{p}_i à effectuer par lesdits premiers moyens de calcul pour calculer chacun des \mathbf{R}_i pour chacun des \mathbf{p}_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo \mathbf{n} ,

- une deuxième entité, appelée dispositif pilote dudit dispositif témoin, pouvant être également contenue notamment dans ledit objet nomade,

ledit dispositif pilote est appelé

* dispositif démonstrateur dans le cas de la preuve de l'authenticité d'une entité ou de l'authenticité d'un message,

* dispositif de signature dans les cas de la preuve de l'origine et de l'intégrité d'un message,

- une troisième entité, appelée dispositif contrôleur, se présentant notamment sous la forme d'un terminal et/ou d'un serveur distant connecté à un réseau de communication informatique,

ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique audit dispositif témoin,

ledit dispositif contrôleur vérifie l'authentification ou l'origine et l'intégrité d'un message,

ledit dispositif témoin reçoit du dispositif pilote ou du dispositif contrôleur, des collections de défis \mathbf{d} $\{\mathbf{dA}, \mathbf{dB}, \dots\}$ tels que $0 \leq \mathbf{dA} \leq \mathbf{v} - 1$, le nombre des collections de défis \mathbf{d} étant égal au nombre d'engagements \mathbf{R} , chaque collection $\{\mathbf{dA}, \mathbf{dB}, \dots\}$ comprenant un nombre de défis égal au nombre de paires de clés,

ledit dispositif témoin comporte des deuxièmes moyens de calcul pour calculer à partir de chacune desdites collections de défis $\{\mathbf{dA}, \mathbf{dB}, \dots\}$ des

réponses **D**

- en effectuant des opérations du type :

$$D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \bmod p_i$$

- puis en appliquant la méthode des restes chinois,

5 de telle sorte qu'il y a autant de réponses **D** que d'engagements **R** et de défis **d**,

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer par lesdits deuxièmes moyens de calcul pour calculer chacun des D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

10

ledit dispositif contrôleur, recevant une ou plusieurs réponses **D**, comporte des troisièmes moyens de calcul pour calculer à partir desdites réponses **D** un engagement **R'** en effectuant des opérations du type :

$$R' \equiv GA^{dA} \cdot GB^{dB} \cdot \dots D' \bmod n$$

15

ou du type :

$$R' \cdot GA^{dA} \cdot GB^{dB} \cdot \dots \equiv D' \bmod n$$

ledit dispositif contrôleur comporte des quatrièmes moyens de calcul pour vérifier que les triplets $\{R', d, D\}$ sont cohérents.

20

13. Système selon la revendication 12 pour diminuer la charge de travail pendant une session destinée à prouver à un contrôleur l'authenticité d'une entité ;

ledit procédé met en œuvre trois entités :

25

1 - une première entité, appelée dispositif témoin, contenue notamment dans un objet nomade se présentant par exemple sous la forme d'une carte bancaire à microprocesseur,

ledit dispositif témoin dispose d'une première zone mémoire contenant des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$,

ledit dispositif témoin dispose aussi d'une deuxième zone mémoire

contenant :

* des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ..., représentant des clés privées QA, QB, \dots

* des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

* un exposant public de vérification v

lesdites paires de clés privées et publiques étant liées par des relations du type :

$$GA \cdot QA^v \bmod n \equiv 1 \text{ ou } GA \equiv QA^v \bmod n$$

2 - une deuxième entité appelée dispositif démonstrateur dudit dispositif témoin, pouvant être également contenue notamment dans ledit objet nomade,

3 - une troisième entité appelée dispositif contrôleur se présentant sous la forme d'un terminal et/ou d'un serveur distant connecté à un réseau de communication informatique,

ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique audit dispositif témoin,

pour prouver l'authenticité d'une entité, ledit dispositif témoin, ledit dispositif démonstrateur et ledit dispositif contrôleur exécutent les étapes suivantes :

• **étape 1. engagement R du dispositif témoin :**

- le dispositif témoin comporte des premiers moyens de calcul pour tirer au hasard et en privé, à chaque appel, au moins une collection de nombres entiers $\{r_1, r_2, r_3, \dots\}$, telle que pour chaque facteur premier p_i , chaque collection comporte un aléa r_i positif et plus petit que p_i ,

- le dispositif témoin comporte des deuxièmes moyens de calcul pour élever chaque aléa r_i à la puissance v ième modulo p_i , pour chaque facteur premier p_i ,

$$R_i \equiv r_i' \pmod{p_i}$$

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer par les deuxièmes moyens de calcul pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

- puis, lesdits deuxièmes moyens de calcul dudit dispositif témoin établissent chaque engagement R modulo n selon la méthode des restes chinois,

de telle sorte qu'il y a autant d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$,

• **étape 2. défi d destiné au dispositif témoin :**

- le dispositif démonstrateur comporte des moyens de transmission pour transmettre tout ou partie de chaque engagement R au dispositif contrôleur,

- le dispositif contrôleur comporte des troisièmes moyens de calcul pour calculer, après avoir reçu tout ou partie de chaque engagement R , au moins une collection de défis d $\{dA, dB, \dots\}$ tels que $0 \leq dA \leq v - 1$, le nombre des collections de défis d étant égal au nombre d'engagements R , chaque collection $\{dA, dB, \dots\}$ comprenant un nombre de défis égal au nombre de paires de clés,

• **étape 3. réponse du dispositif témoin au défi d :**

- ledit dispositif témoin comporte des quatrièmes moyens de calcul pour calculer des réponses D , à partir desdites collections de défis d $\{dA, dB, \dots\}$ reçues du dispositif contrôleur,

en effectuant des opérations du type :

$$D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \pmod{p_i}$$

puis en appliquant la méthode des restes chinois,

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer par les quatrièmes moyens de calcul pour calculer chacun des D_i pour

chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

de telle sorte qu'il y a autant de réponses D calculées par le témoin que d'engagements R et de défis d ,

5 • **étape 4. données destinées au dispositif contrôleur :**

- le démonstrateur comporte des moyens de transmission pour transmettre au dispositif contrôleur chaque réponse D ,

 • **étape 5. vérification par le dispositif contrôleur :**

10 ledit dispositif contrôleur comporte des cinquièmes moyens de calcul pour calculer à partir de chaque réponse D un engagement R' en effectuant des opérations du type :

$$R' \equiv GA^{d_A} \cdot GB^{d_B} \cdot \dots D^v \text{ mod } n$$

ou du type :

$$R' \cdot GA^{d_A} \cdot GB^{d_B} \cdot \dots \equiv D^v \text{ mod } n$$

15 ledit dispositif contrôleur comporte des sixièmes moyens de calcul pour comparer et vérifier que chaque engagement reconstruit R' reproduit tout ou partie de chaque engagement R transmis à l'étape 2 par le dispositif démonstrateur.

20 14. Système selon la revendication 12 pour diminuer la charge de travail pendant une session destinée à prouver à un contrôleur l'authenticité d'un message m ,

ledit procédé met en œuvre trois entités :

25 1 - une première entité appelée dispositif témoin, contenue notamment dans un objet nomade se présentant par exemple sous la forme d'une carte bancaire à microprocesseur,

ledit dispositif témoin dispose d'une première zone mémoire contenant des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$,

ledit dispositif témoin dispose aussi d'une deuxième zone mémoire

contenant

* des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ..., représentant des clés privées QA, QB, \dots

* des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

* un exposant public de vérification v

lesdites paires de clés privées et publiques étant liées par des relations du type :

$$GA \cdot QA' \bmod n \equiv 1 \text{ ou } GA \equiv QA' \bmod n$$

2 - une deuxième entité, appelée démonstrateur dudit dispositif témoin, pouvant être également contenue notamment dans ledit objet nomade,

3 - une troisième entité appelée dispositif contrôleur se présentant sous la forme d'un terminal et/ou d'un serveur distant connecté à un réseau de communication informatique,

ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique audit dispositif témoin,

pour prouver l'authenticité d'un message ledit dispositif témoin, ledit dispositif démonstrateur et ledit dispositif contrôleur exécutent les étapes suivantes :

• **étape 1. engagement R du dispositif témoin :**

- ledit dispositif témoin comporte des premiers moyens de calcul pour tirer au hasard et en privé, à chaque appel, au moins une collection de nombres entiers $\{r_1, r_2, r_3, \dots\}$, telle que pour chaque facteur premier p_i , chaque collection comporte un aléa r_i positif et plus petit que p_i ,

- ledit dispositif témoin comporte des deuxièmes moyens de calcul pour élever chaque aléa r_i à la puissance v ième modulo p_i , pour chaque facteur premier p_i ,

$$R_i \equiv r_i^v \bmod p_i$$

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer par les deuxièmes moyens de calcul pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

- puis, lesdits deuxièmes moyens de calcul dudit dispositif témoin établissent chaque engagement R modulo n selon la méthode des restes chinois,

de telle sorte qu'il y a autant d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$,

• **étape 2. défi d destiné au dispositif témoin :**

- le dispositif démonstrateur comporte des premiers moyens de calcul pour calculer, en appliquant une fonction de hachage f ayant comme arguments le message m et chaque engagement R pour un jeton T ,

- ledit dispositif démonstrateur comporte des moyens de transmission pour transmettre le jeton T au dispositif contrôleur

- ledit dispositif contrôleur comporte des troisièmes moyens de calcul pour calculer, après avoir reçu le jeton T , au moins une collection de défis d $\{dA, dB, \dots\}$ tels que $0 \leq dA \leq v - 1$, le nombre des collections de défis d étant égal au nombre d'engagements R , chaque collection $\{dA, dB, \dots\}$ comprenant un nombre de défis égal au nombre de paires de clés,

• **étape 3. réponse du dispositif témoin au défi d :**

- ledit dispositif témoin comporte des quatrièmes moyens de calcul pour calculer des réponses D , à partir desdites collection de défis d $\{dA, dB, \dots\}$ reçues du dispositif contrôleur

en effectuant des opérations du type :

$$D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \bmod p_i$$

puis en appliquant la méthode des restes chinois,

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer

par les quatrièmes moyens de calcul pour calculer chacun des D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

de telle sorte qu'il y a autant de réponses D calculées par le témoin que d'engagements R et de défis d ,

• **étape 4. données destinées au dispositif contrôleur :**

- le démonstrateur comporte des moyens de transmission pour transmettre au dispositif contrôleur chaque réponse D ,

• **étape 5. vérification par le dispositif contrôleur :**

ledit dispositif contrôleur comporte des cinquièmes moyens de calcul pour calculer à partir de chaque réponse D un engagement R' en effectuant des opérations du type :

$$R' \equiv GA^{dA} \cdot GB^{dB} \cdot \dots D^v \text{ mod } n$$

ou du type :

$$R' \cdot GA^{dA} \cdot GB^{dB} \cdot \dots \equiv D^v \text{ mod } n$$

ledit dispositif contrôleur comporte des sixièmes moyens de calcul pour calculer, en appliquant la fonction de hachage f ayant comme arguments le message m et chaque engagement R' , le jeton T' ,

ledit dispositif contrôleur comporte des septièmes moyens de calcul pour comparer et vérifier que le jeton T' est identique au jeton T transmis à l'étape 2 par le dispositif démonstrateur.

15. Système selon la revendication 12 pour diminuer la charge de travail pendant une session destinée à prouver à un contrôleur la signature numérique d'un message m ,

ledit procédé met en œuvre trois entités :

1 - une première entité, appelée dispositif témoin, contenues notamment dans un objet nomade se présentant par exemple sous la forme d'une carte bancaire à microprocesseur,

ledit dispositif témoin comporte une première zone mémoire contenant des

facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$,

ledit dispositif témoin comporte aussi une deuxième zone mémoire contenant :

5 * des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ..., représentant des clés privées QA, QB, \dots

 * des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

 * un exposant publique de vérification v

10 lesdites paires de clés privées et publiques étant liés par des relations du type :

$$GA \cdot QA^v \bmod n \equiv 1 \text{ ou } GA \equiv QA^v \bmod n$$

2 - une deuxième entité appelée dispositif de signature, pouvant être également contenue notamment dans ledit objet nomade,

15 3 - une troisième entité appelée dispositif contrôleur se présentant sous la forme d'un terminal et/ou d'un serveur distant connecté à un réseau de communication informatique,

ledit dispositif contrôleur comporte des moyens de connexion pour le connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique audit dispositif témoin,

20 pour prouver la signature d'un message ledit dispositif témoin, ledit dispositif démonstrateur et ledit dispositif contrôleur exécutent les étapes suivantes :

• **étape 1. engagement R du témoin :**

- 25 - le dispositif témoin comporte des premiers moyens de calcul pour tirer au hasard et en privé, à chaque appel, au moins une collection de nombres entiers $\{r_1, r_2, r_3, \dots\}$, telle que pour chaque facteur premier p_i , chaque collection comporte un aléa r_i positif et plus petit que p_i ,
- le dispositif témoin comporte des deuxième moyens de calcul pour élever

chaque aléa r_i à la puissance v ième modulo p_i , pour chaque facteur premier p_i ,

$$R_i \equiv r_i^v \text{ mod } p_i$$

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer par les deuxièmes moyens de calcul pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

- puis, lesdits deuxièmes moyens de calcul dudit dispositif témoin établissent chaque engagement R modulo n selon la méthode des restes chinois,

de telle sorte qu'il y a autant d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$,

• **étape 2. défi d destiné au dispositif témoin :**

- ledit dispositif de signature comporte des troisièmes moyens de calcul pour calculer, en appliquant une fonction de hachage f ayant comme arguments le message m et chaque engagement R , au moins une collection de défis d $\{dA, dB, \dots\}$ tels que $0 \leq dA \leq v - 1$, le nombre des collections de défis d étant égal au nombre d'engagements R , chaque collection $\{dA, dB, \dots\}$ comprenant un nombre de défis égal au nombre de paires de clés,

- le dispositif de signature transmet les collections de défis d au témoin,

• **étape 3. réponse du dispositif témoin au défi d :**

- ledit dispositif témoin comporte des quatrièmes moyens de calcul pour calculer des réponses D , à partir desdites collections de défis d $\{dA, dB, \dots\}$ reçues du dispositif contrôleur,

en effectuant des opérations du type :

$$D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \text{ mod } p_i$$

puis en appliquant la méthode des restes chinois,

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer

par les quatrièmes moyens de calcul pour calculer chacun des D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

de telle sorte qu'il y a autant de réponses D calculées par le témoin que d'engagements R et de défis d ,

5

- ledit dispositif témoin comporte des moyens de transmission pour transmettre les réponses D au dispositif de signature et/ou au dispositif contrôleur,

• **étape 4. données destinées au dispositif contrôleur :**

10

- le dispositif de signature transmet au dispositif contrôleur un message signé comprenant :

/ le message m ,

/ les collections de défis d ou les engagements R ,

/ chaque réponse D

15

• **étape 5. vérification par le dispositif contrôleur :**

cas où le dispositif contrôleur reçoit la collection des défis d ,

dans le cas où le dispositif contrôleur reçoit les collections des défis d et des réponses D , ledit dispositif contrôleur comporte des cinquièmes moyens de calcul pour calculer à partir de chaque réponse D un engagement R' en effectuant des opérations du type :

20

$$R' \equiv GA^{d_A} \cdot GB^{d_B} \cdot \dots D' \bmod n$$

ou du type :

$$R' \cdot GA^{d_A} \cdot GB^{d_B} \cdot \dots \equiv D' \bmod n$$

ledit dispositif contrôleur comporte des sixièmes moyens de calcul pour calculer chaque défi d' , en appliquant la fonction de hachage f ayant comme arguments le message m et chaque engagement reconstruit R' ,

25

ledit dispositif contrôleur comporte des septièmes moyens de calcul pour comparer et vérifier que chaque défi d' est identique au défi d figurant dans le message signé,

cas où le dispositif contrôleur reçoit la collection des engagements R

dans le cas où le dispositif contrôleur reçoit la collection des engagements **R** et des réponses **D**, ledit dispositif contrôleur comporte des cinquièmes moyens de calcul pour calculer chaque défi **d'**, en appliquant la fonction de hachage **f** ayant comme arguments le message **m** et chaque engagement **R**,
 5 ledit dispositif contrôleur comporte des sixièmes moyens de calcul pour calculer alors la collection des engagements **R'** en effectuant des opérations du type

$$R' \equiv GA^{d'A} \cdot GB^{d'B} \cdot \dots D' \bmod n$$

10 ou du type :

$$R' \cdot GA^{d'A} \cdot GB^{d'B} \cdot \dots \equiv D' \bmod n$$

ledit dispositif contrôleur comporte des septièmes moyens de calcul pour comparer et vérifier que chaque engagement **R'** reconstruit est identique à l'engagement **R** figurant dans le message signé.

15 **16.** Système selon l'une quelconque des revendications 11 à 15 tel que les composantes **QA₁, QA₂, ... (QA_i, ...)**, et **QB₁, QB₂, ... (QB_i, ...)**, ... des clés privées **QA, QB, ...** sont des nombres tirés au hasard à raison d'une composante **QA_i, QB_i, ...** pour chacun desdits facteurs premiers **p_i**, lesdites clés privées **QA, QB**, pouvant être calculées à partir desdites composantes **QA₁, QA₂, ... (QA_i, ...)**, et **QB₁, QB₂, ... (QB_i, ...)**, ... par la
 20 méthode des restes chinois,

ledit dispositif témoin comportant des huitièmes moyens de calcul pour calculer lesdites clés publiques **GA, GB, ...**,

• en effectuant des opérations du type :

$$GA_i \equiv QA_i' \bmod p_i$$

• puis en appliquant la méthode des restes chinois pour établir **GA** tel que

$$GA \equiv QA' \bmod n$$

ou bien tel que

$$GA \cdot QA' \bmod n \equiv 1$$

5

10

$$\mathbf{v} = \mathbf{a}^k$$

15

$$\mathbf{v} = 2^{\mathbf{k}}$$

20

$$\mathbf{x}^2 \equiv \mathbf{gA} \bmod n \quad \text{et} \quad \mathbf{x}^2 \equiv -\mathbf{gA} \bmod n$$

25

$$GA \equiv QA_i^{2\exp(k)} \bmod p_i$$

$$GA \cdot QA_i^{2 \cdot \exp(k)} \bmod p_i \equiv 1$$

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer

par les neuvièmes moyens de calcul du dispositif témoin pour calculer chacun des QA_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,
de sorte que la paire de clés GA , QA confère une sécurité équivalente à la connaissance de la factorisation de n .

20. Système selon la revendication 19 tel que pour extraire la k ième racine carrée de GA dans le corps de Galois $CG(p_i)$,

* dans le cas où le facteur premier p_i est congru à 3 modulo 4, les neuvièmes moyens de calcul du dispositif témoin appliquent notamment un algorithme du type :

$$x = (p+1)/4 ; y \equiv x^k \text{ mod } (p-1) ; z = y ; QA_i \equiv GA^z \text{ mod } p_i$$

* dans le cas où le facteur premier p_i est congru à 1 modulo 4, les neuvièmes moyens de calcul du dispositif témoin appliquent notamment un algorithme basé sur les suites de Lucas.

21. Objet nomade, se présentant par exemple sous la forme d'une carte bancaire à microprocesseur, pour diminuer la charge de travail pendant une session destinée à prouver à un serveur contrôleur,

- l'authenticité d'une entité et/ou
- l'origine et l'intégrité d'un message m ,

ledit objet nomade faisant intervenir trois entités :

- une première entité, appelée dispositif témoin, contenue dans ledit objet nomade,

ledit dispositif témoin dispose d'une première zone mémoire contenant des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$,

ledit dispositif témoin dispose aussi d'une deuxième zone mémoire contenant :

* des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ..., représentant des clés privées QA, QB, \dots

* des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

* des exposants publics de vérification vx, vy, \dots

lesdites clés privées et clés publiques étant liées par des relations du type :

5

$$GA \cdot QA^{vx} \bmod n \equiv 1 \text{ ou } GA \equiv QA^{vx} \bmod n$$

ledit dispositif témoin comporte aussi des premiers moyens de calcul pour calculer des engagements R en effectuant des opérations du type :

$$R_i \equiv r_i^{vx} \bmod p_i$$

où r_i est un aléa tel que $0 < r_i < p_i$,

10

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer par lesdits premiers moyens de calcul pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

15

- une deuxième entité, appelée dispositif pilote dudit dispositif témoin, pouvant être également contenue dans ledit objet nomade,

ledit dispositif pilote est appelé

* dispositif démonstrateur dans le cas de la preuve de l'authenticité d'une entité ou de l'authenticité d'un message,

20

* dispositif de signature dans les cas de la preuve de l'origine et de l'intégrité d'un message,

- une troisième entité appelée dispositif contrôleur se présentant notamment sous la forme d'un terminal et/ou d'un serveur distant connecté à un réseau de communication informatique,

25

ledit dispositif contrôleur vérifie l'authentification ou l'origine et l'intégrité d'un message,

ledit objet nomade comporte des moyens de connexion pour connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique ledit dispositif témoin et/ou ledit dispositif pilote audit dispositif contrôleur,

ledit dispositif témoin reçoit du dispositif pilote ou du dispositif contrôleur un ou plusieurs défis d tel que $0 \leq d \leq vx - 1$ et comporte des deuxièmes moyens de calcul pour calculer à partir dudit défi d une ou plusieurs réponses D en effectuant des opérations du type :

$$5 \quad D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \bmod p_i$$

où r_i est un entier, associé au nombre premier p_i , tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, r_3, \dots\}$,

le témoin tire au hasard une ou plusieurs collections d'aléas de telle sorte que, pour chaque exposant public de vérification v , il y a autant
10 d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$,

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer par lesdits deuxièmes moyens de calcul pour calculer chacune des réponses D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

15 ledit objet nomade comporte des moyens de transmission pour transmettre audit dispositif contrôleur la ou les dites réponses D .

22. Objet nomade se présentant par exemple sous la forme d'une carte bancaire à microprocesseur, pour diminuer la charge de travail pendant une session destinée à prouver à un contrôleur,

- 20
- l'authenticité d'une entité et/ou
 - l'origine et l'intégrité d'un message m ,

ledit objet nomade faisant intervenir trois entités:

- une première entité, appelée dispositif témoin, contenue dans ledit objet nomade,

25 ledit dispositif témoin dispose d'une première zone mémoire contenant des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$,

ledit dispositif témoin dispose aussi d'une deuxième zone mémoire contenant

* des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ..., représentant des clés privées QA, QB, \dots

* des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

5 * un exposant public de vérification v

lesdites paires de clés privées et publiques étant liées par des relations du type :

$$GA \cdot QA^v \bmod n \equiv 1 \text{ ou } GA \equiv QA^v \bmod n$$

10 ledit dispositif témoin comporte aussi des premiers moyens de calcul pour calculer des engagements R_i ,

• en effectuant des opérations du type :

$$R_i \equiv r_i^v \bmod p_i$$

où r_i est un entier, tiré au hasard, associé au nombre premier p_i , tel que $0 < r_i < p_i$, chaque r_i appartenant à une collection d'aléas $\{r_1, r_2, r_3, \dots\}$,

15 • puis en appliquant la méthode des restes chinois,

le témoin tire au hasard une ou plusieurs collections d'aléas de telle sorte qu'il y a autant d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$, de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer par lesdits premiers moyens de calcul pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

20

- une deuxième entité, appelée dispositif pilote dudit dispositif témoin, pouvant être également contenue dans ledit objet nomade, ledit dispositif pilote est appelé

25

* dispositif démonstrateur dans le cas de la preuve de l'authenticité d'une entité ou de l'authenticité d'un message,

* dispositif de signature dans le cas de la preuve de l'origine et de l'intégrité d'un message,

- une troisième entité, appelée dispositif contrôleur, se présentant

notamment sous la forme d'un terminal et/ou d'un serveur distant connecté à un réseau de communication informatique,

ledit dispositif contrôleur vérifie l'authentification ou l'origine et l'intégrité d'un message,

5 ledit objet nomade comporte des moyens de connexion pour connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique ledit dispositif témoin et/ou ledit dispositif pilote audit dispositif contrôleur,

10 ledit dispositif témoin reçoit du dispositif pilote ou du dispositif contrôleur, des collections de défis \mathbf{d} $\{\mathbf{dA}, \mathbf{dB}, \dots\}$ tels que $0 \leq \mathbf{dA} \leq v - 1$, le nombre des collections de défis \mathbf{d} étant égal au nombre d'engagements \mathbf{R} , chaque collection $\{\mathbf{dA}, \mathbf{dB}, \dots\}$ comprenant un nombre de défis égal au nombre de paires de clés,

15 ledit dispositif témoin comporte des deuxièmes moyens de calcul pour calculer à partir de chacune desdites collections de défis $\{\mathbf{dA}, \mathbf{dB}, \dots\}$ des réponses \mathbf{D}

- en effectuant des opérations du type :

$$D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \dots \text{mod } p_i$$

20 • puis en appliquant la méthode des restes chinois, de telle sorte qu'il y a autant de réponses \mathbf{D} que d'engagements \mathbf{R} et de défis \mathbf{d} ,

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer par lesdits deuxièmes moyens de calcul pour calculer chacun des \mathbf{D}_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

25 ledit objet nomade comporte des moyens de transmission pour transmettre audit dispositif contrôleur la ou lesdites réponses \mathbf{D} .

23. Objet nomade selon la revendication 22 pour diminuer la charge de travail pendant une session destinée à prouver à un dispositif contrôleur

l'authenticité d'une entité ;

ledit objet nomade faisant intervenir trois entités :

1 - une première entité, appelée dispositif témoin, contenue dans ledit objet nomade,

5 ledit dispositif témoin comporte une première zone mémoire contenant des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$,

ledit dispositif témoin comporte aussi une deuxième zone mémoire contenant :

10 * des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ..., représentant des clés privées QA, QB, \dots

* des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

* un exposant public de vérification v

15 lesdites paires de clés privées et publiques étant liées par des relations du type :

$$GA \cdot QA^v \bmod n \equiv 1 \text{ ou } GA \equiv QA^v \bmod n$$

20 2 - une deuxième entité, appelée dispositif démonstrateur dudit dispositif témoin, pouvant être également contenue dans ledit objet nomade,

3 - une troisième entité appelée dispositif contrôleur se présentant notamment sous la forme d'un terminal et/ou d'un serveur distant connecté à un réseau de communication informatique,

25 ledit objet nomade comporte des moyens de connexion pour connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique ledit dispositif témoin et/ou ledit dispositif démonstrateur audit dispositif contrôleur,

pour prouver l'authenticité d'une entité, ledit objet nomade exécute les étapes suivantes :

• **étape 1. engagement R du dispositif témoin :**

- le dispositif témoin comporte des premiers moyens de calcul pour tirer au hasard et en privé, à chaque appel, au moins une collection de nombres entiers $\{r_1, r_2, r_3, \dots\}$, telle que pour chaque facteur premier p_i , chaque collection comporte un aléa r_i positif et plus petit que p_i ,

- le dispositif témoin comporte des deuxièmes moyens de calcul pour élever chaque aléa r_i à la puissance v ième modulo p_i , pour chaque facteur premier p_i ,

$$R_i \equiv r_i^v \pmod{p_i}$$

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer par les deuxièmes moyens de calcul pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

- puis, lesdits deuxièmes moyens de calcul dudit dispositif témoin établissent chaque engagement R modulo n selon la méthode des restes chinois,

de telle sorte qu'il y a autant d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$,

• **étape 2. transmission des engagements R et réception des défis d destinés au dispositif témoin :**

- ledit objet nomade comporte des moyens de transmission pour transmettre au dispositif contrôleur tout ou partie de chaque engagement R ,

- ledit objet nomade comporte des moyens de réception pour recevoir des collections de défis d $\{dA, dB, \dots\}$ produits par ledit dispositif contrôleur,

• **étape 3. réponse du dispositif témoin aux défis d :**

- ledit dispositif témoin comporte des troisièmes moyens de calcul pour calculer des réponses D , à partir desdites collections de défis d $\{dA, dB, \dots\}$ reçues du dispositif contrôleur, en effectuant des opérations du type :

$$D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \bmod p_i$$

puis en appliquant la méthode des restes chinois,

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer par les troisièmes moyens de calcul pour calculer chacun des D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

de telle sorte qu'il y a autant de réponses D calculées par le témoin que d'engagements R et de défis d ,

• **étape 4. données destinées au dispositif contrôleur :**

- ledit objet nomade comporte des moyens de transmission pour transmettre au dispositif contrôleur chaque réponse D ,

• **étape 5. vérification par le dispositif contrôleur :**

ledit dispositif contrôleur vérifie la cohérence des triplets $\{R, d, D\}$ et l'authenticité de l'entité contrôlée.

24. Objet nomade selon la revendication 22 pour diminuer la charge de travail pendant une session destinée à prouver à un contrôleur l'authenticité d'un message m ,

ledit objet nomade faisant intervenir trois entités :

1 - une première entité, appelée dispositif témoin, contenue dans ledit objet nomade,

ledit dispositif témoin comporte une première zone mémoire contenant des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$,

ledit dispositif témoin comporte aussi une deuxième zone mémoire contenant

* des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ..., représentant des clés privées QA, QB, \dots

* des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

* un exposant public de vérification v

lesdites paires de clés privées et publiques étant liées par des relations du type :

$$GA.QA' \bmod n \equiv 1 \text{ ou } GA \equiv QA' \bmod n$$

5 2 - une deuxième entité, appelée démonstrateur dudit dispositif témoin, pouvant être également contenue dans ledit objet nomade,

3 - une troisième entité appelée dispositif contrôleur se présentant sous la forme d'un terminal et/ou d'un serveur distant connecté à un réseau de communication informatique,

10 ledit objet nomade comporte des moyens de connexion pour connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique ledit dispositif témoin et/ou ledit dispositif démonstrateur audit dispositif contrôleur,

15 pour prouver l'authenticité d'un message ledit objet nomade exécute les étapes suivantes :

• **étape 1. engagement R du dispositif témoin :**

20 - ledit dispositif témoin comporte des premiers moyens de calcul pour tirer au hasard et en privé, à chaque appel, au moins une collection de nombres entiers $\{r_1, r_2, r_3, \dots\}$, telle que, pour chaque facteur premier p_i , chaque collection comporte un aléa r_i positif et plus petit que p_i ,

- ledit dispositif témoin comporte des deuxièmes moyens de calcul pour élever chaque aléa r_i à la puissance v ième modulo p_i , pour chaque facteur premier p_i ,

$$R_i \equiv r_i^v \bmod p_i$$

25 (de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer par les deuxièmes moyens de calcul pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

- puis, lesdits deuxièmes moyens de calcul dudit dispositif témoin

établissent chaque engagement R modulo n selon la méthode des restes chinois,

de telle sorte qu'il y a autant d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$,

5 • **étape 2. réception des défis d destinés au dispositif témoin:**

- le dispositif démonstrateur comporte des premiers moyens de calcul pour calculer, en appliquant une fonction de hachage f ayant comme arguments le message m et chaque engagement R pour un jeton T ,

10 - ledit objet nomade comporte des moyens de transmission pour transmettre audit dispositif contrôleur le jeton T ,

- ledit objet nomade comporte des moyens de réception pour recevoir des collections de défis d $\{dA, dB, \dots\}$ produits par ledit dispositif contrôleur au moyen du jeton T ,

 • **étape 3. réponse du dispositif témoin au défi d :**

15 - ledit dispositif témoin comporte des troisièmes moyens de calcul pour calculer des réponses D , à partir desdites collections de défis d $\{dA, dB, \dots\}$ reçues du dispositif contrôleur

en effectuant des opérations du type :

$$D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \bmod p_i$$

20 puis en appliquant la méthode des restes chinois,
de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer par les quatrièmes moyens de calcul pour calculer chacun des D_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

25 de telle sorte qu'il y a autant de réponses D calculées par le témoin que d'engagements R et de défis d ,

 • **étape 4. données destinées au dispositif contrôleur :**

- l'objet nomade comporte des moyens de transmission pour transmettre audit dispositif contrôleur chaque réponse D

• **étape 5. vérification par le dispositif contrôleur :**

ledit dispositif contrôleur vérifie la cohérence des triplets $\{R, d, D\}$ et l'authenticité du message m .

5 **25.** Objet nomade selon la revendication 22 pour diminuer la charge de travail pendant une session destinée à prouver à un contrôleur la signature numérique d'un message m ,

ledit objet nomade faisant intervenir trois entités :

1 - une première entité, appelée dispositif témoin, contenue dans ledit objet nomade,

10 ledit dispositif témoin comporte une première zone mémoire contenant des facteurs premiers $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2) d'un module public n tel que $n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$,

ledit dispositif témoin comporte aussi une deuxième zone mémoire contenant :

15 * des composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ..., représentant des clés privées QA, QB, \dots

* des clés publiques GA, GB, \dots ayant respectivement pour composantes $GA_1, GA_2, \dots (GA_i, \dots)$ et $GB_1, GB_2, \dots (GB_i, \dots)$

* un exposant public de vérification v

20 lesdites paires de clés privées et publiques étant liées par des relations du type :

$$GA \cdot QA^v \bmod n \equiv 1 \text{ ou } GA \equiv QA^v \bmod n$$

2 - une deuxième entité appelée dispositif de signature, pouvant être également contenue dans ledit objet nomade,

25 3 - une troisième entité appelée dispositif contrôleur se présentant sous la forme d'un terminal et/ou d'un serveur distant connecté à un réseau de communication informatique,

ledit objet nomade comporte des moyens de connexion pour connecter électriquement, électromagnétiquement, optiquement ou de manière

acoustique ledit dispositif témoin et ledit dispositif de signature audit dispositif contrôleur,

pour prouver la signature d'un message ledit objet nomade exécute les étapes suivantes :

5 • **étape 1. engagement R du dispositif témoin :**

- le dispositif témoin comporte des premiers moyens de calcul pour tirer au hasard et en privé, à chaque appel, au moins une collection de nombres entiers $\{r_1, r_2, r_3, \dots\}$, telle que pour chaque facteur premier p_i , chaque collection comporte un aléa r_i positif et plus petit que p_i ,

10 - le dispositif témoin comporte des deuxièmes moyens de calcul pour élever chaque aléa r_i à la puissance v ième modulo p_i , pour chaque facteur premier p_i ,

$$R_i \equiv r_i^v \text{ mod } p_i$$

15 de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer par les deuxièmes moyens de calcul pour calculer chacun des R_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

20 - puis, lesdits deuxièmes moyens de calcul dudit dispositif témoin établissent chaque engagement R modulo n selon la méthode des restes chinois,

de telle sorte qu'il y a autant d'engagements R que de collections d'aléas $\{r_1, r_2, r_3, \dots\}$,

 • **étape 2. défi d destiné au dispositif témoin :**

25 - ledit dispositif de signature comporte des troisièmes moyens de calcul pour calculer, en appliquant une fonction de hachage f ayant comme arguments le message m et chaque engagement R , au moins une collection de défis d $\{dA, dB, \dots\}$ tels que $0 \leq dA \leq v - 1$, le nombre des collections de défis d étant égal au nombre d'engagements R , chaque collection $\{dA, dB, \dots\}$ comprenant un nombre de défis égal au nombre de paires de clés,

- le dispositif de signature transmet les collections de défis **d** au témoin,

• **étape 3. réponse du dispositif témoin au défi d :**

- ledit dispositif témoin comporte des quatrièmes moyens de calcul pour calculer des réponses **D**, à partir desdites collections de défis **d** {**dA**, **dB**, ...} reçues du dispositif contrôleur,

en effectuant des opérations du type :

$$D_i \equiv r_i \cdot QA_i^{dA} \cdot QB_i^{dB} \cdot \dots \bmod p_i$$

puis en appliquant la méthode des restes chinois,

de sorte que le nombre d'opérations arithmétiques modulo **p_i** à effectuer par les quatrièmes moyens de calcul pour calculer chacun des **D_i** pour chacun des **p_i** est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo **n**,

de telle sorte qu'il y a autant de réponses **D** calculées par le témoin que d'engagements **R** et de défis **d**,

- l'objet nomade comporte des moyens de transmission pour transmettre les réponses **D** au dispositif de signature et/ou au dispositif contrôleur,

• **étape 4. données destinées au dispositif contrôleur :**

- l'objet nomade comporte des moyens de transmission pour transmettre au dispositif contrôleur un message signé comprenant :

/ le message **m**,

/ les collections de défis **d** ou les engagements **R**,

/ chaque réponse **D**

• **étape 5. vérification par le dispositif contrôleur :**

ledit dispositif contrôleur vérifie la cohérence des triplets {**R**, **d**, **D**} et la signature numérique du message **m**.

26. Objet nomade selon l'une quelconque des revendications 21 à 25 tel que les composantes **QA₁**, **QA₂**, ... (**QA_i**, ...), et **QB₁**, **QB₂**, ... (**QB_i**, ...), ... des clés privées **QA**, **QB**, ... sont des nombres tirés au hasard à raison d'une composante **QA_i**, **QB_i**, ... pour chacun desdits facteurs

premiers p_i , lesdites clés privées QA , QB , pouvant être calculées à partir desdites composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, par la méthode des restes chinois,

ledit dispositif témoin comportant des huitièmes moyens de calcul pour calculer lesdites clés publiques GA, GB, \dots ,

5

- en effectuant des opérations du type :

$$GA_i \equiv QA_i' \bmod p_i$$

- puis en appliquant la méthode des restes chinois pour établir GA tel que

$$GA \equiv QA' \bmod n$$

10

ou bien tel que

$$GA.QA' \bmod n \equiv 1$$

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer par les huitièmes moyens de calcul dudit dispositif témoin pour calculer chacun des GA_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

15

27. Objet nomade selon la revendication 26 tel que l'exposant public de vérification v est un nombre premier, de sorte que la paire de clés GA, QA confère une sécurité équivalente à la connaissance de la clé privée QA .

20

28. Objet nomade selon l'une quelconque des revendications 21 à 25 tel que l'exposant public de vérification v est du type

$$v = a^k$$

où k est un paramètre de sécurité plus grand que 1.

29. Objet nomade selon la revendication 28 tel que :

25

- l'exposant public de vérification v est du type

$$v = 2^k$$

où k est un paramètre de sécurité plus grand que 1,

- la clé publique GA est un carré gA^2 inférieur à n choisi de telle sorte que les deux équations

$$x^2 \equiv gA \bmod n \quad \text{et} \quad x^2 \equiv -gA \bmod n$$

n'ont pas de solution en x dans l'anneau des entiers modulo n

- ledit dispositif témoin comportant des neuvièmes moyens de calcul pour calculer lesdites composantes $QA_1, QA_2, \dots (QA_i, \dots)$ de la clé privée QA en appliquant des formules telles que :

$$GA \equiv QA_i^{2 \cdot \exp(k)} \bmod p_i$$

ou bien telles que :

$$GA \cdot QA_i^{2 \cdot \exp(k)} \bmod p_i \equiv 1$$

et en extrayant la k ième racine carrée de GA dans le corps de Galois $CG(p_i)$,

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer par les neuvièmes moyens de calcul du dispositif témoin pour calculer chacun des QA_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

de sorte que la paire de clés GA, QA confère une sécurité équivalente à la connaissance de la factorisation de n .

30. Objet nomade selon la revendication 29 tel que pour extraire la k ième racine carrée de GA dans le corps de Galois $CG(p_i)$,

* dans le cas où le facteur premier p_i est congru à 3 modulo 4, les neuvièmes moyens de calcul du dispositif témoin appliquent notamment un algorithme du type :

$$x = (p+1)/4 ; y \equiv x^k \bmod (p-1) ; z = y ; QA_i \equiv GA^z \bmod p_i$$

* dans le cas où le facteur premier p_i est congru à 1 modulo 4, les neuvièmes moyens de calcul du dispositif témoin appliquent notamment un algorithme basé sur les suites de Lucas.

31. Dispositif de contrôle permettant de diminuer la charge de travail pendant une session destinée à vérifier :

- l'authenticité d'une entité et/ou
- l'origine et l'intégrité d'un message m ,

ledit dispositif de contrôle se présentant sous la forme d'un terminal ou d'un serveur distant connecté à un réseau de communication informatique, ledit dispositif de contrôle mettant en œuvre :

- un module public n tel que n soit le produit de facteurs premiers secrets $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2)

$$n = p_1 \cdot p_2 \cdot p_3 \cdot \dots ,$$

- des clés publiques GA, GB, \dots

- des exposants publics de vérification vx, vy, \dots

lesdites clés privées GA et les clés publiques associées QA étant liées par des relations du type :

$$GA \cdot QA^{vx} \bmod n \equiv 1 \text{ ou } GA \equiv QA^{vy} \bmod n$$

ledit dispositif de contrôle faisant intervenir trois entités :

- une première entité, appelée dispositif témoin, contenue notamment dans un objet nomade se présentant par exemple sous la forme d'une carte bancaire à microprocesseur, ledit dispositif témoin produisant des engagements R ,

- une deuxième entité appelée dispositif pilote dudit dispositif témoin pouvant être contenue notamment dans ledit objet nomade,

- une troisième entité, appelée dispositif contrôleur, contenue dans ledit dispositif de contrôle,

ledit dispositif de contrôle comporte :

- des moyens de connexion pour connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique ledit dispositif contrôleur audit dispositif témoin et/ou audit dispositif pilote,

- des moyens de transmission pour transmettre les données produites par ledit dispositif contrôleur vers ledit dispositif témoin et/ou ledit dispositif pilote,

- des moyens de réception pour recevoir les données provenant dudit dispositif témoin et/ou dudit dispositif pilote,

ledit dispositif contrôleur comporte :

- des premiers moyens de calcul pour produire un ou plusieurs défis d tel que $0 \leq d \leq vx - 1$,

- des deuxièmes moyens de calcul pour calculer, en fonction des réponses D reçues dudit dispositif témoin et/ou dudit dispositif pilote, des engagements R' , en effectuant des opérations du type :

$$R'_i \equiv GA^d \cdot D^{v_i} \mod n$$

ou du type :

$$R'_i \cdot GA^d \equiv D^{v_i} \mod n$$

- des troisièmes moyens de calcul pour vérifier que les triplets $\{R', d, D\}$ sont cohérents

32. Dispositif de contrôle permettant de diminuer la charge de travail pendant une session destinée à vérifier,

- l'authenticité d'une entité et/ou

- l'origine et l'intégrité d'un message m ,

ledit dispositif de contrôle se présentant sous la forme d'un terminal ou d'un serveur distant connecté à un réseau de communication informatique, ledit dispositif de contrôle mettant en œuvre :

- un module public n tel que n soit le produit de facteurs premiers secrets $p_1, p_2, \dots (p_i, \dots)$ (i étant supérieur ou égal à 2)

$$n = p_1 \cdot p_2 \cdot p_3 \cdot \dots$$

- des clés publiques GA, GB, \dots

- un exposant public de vérification v

lesdites clés privées GA et les clés publiques associées QA étant liées par des relations du type :

$$GA \cdot QA^v \mod n \equiv 1 \text{ ou } GA \equiv QA^v \mod n$$

ledit dispositif de contrôle faisant intervenir trois entités :

- une première entité, appelée dispositif témoin, contenue notamment dans un objet nomade se présentant par exemple sous la forme d'une carte

bancaire à microprocesseur, ledit dispositif témoin produisant des engagements R ,

- une deuxième entité, appelée dispositif pilote dudit dispositif témoin, pouvant être contenue notamment dans ledit objet nomade,

5 - une troisième entité, appelée dispositif contrôleur, contenue dans ledit dispositif de contrôle,

ledit dispositif de contrôle comporte :

- des moyens de connexion pour connecter électriquement, électromagnétiquement, optiquement ou de manière acoustique ledit

10 dispositif contrôleur audit dispositif témoin et/ou audit dispositif pilote,

- des moyens de transmission pour transmettre les données produites par ledit dispositif contrôleur vers ledit dispositif témoin et/ou ledit dispositif pilote,

15 - des moyens de réception pour recevoir les données provenant dudit dispositif témoin et/ou dudit dispositif pilote,

ledit dispositif contrôleur comporte :

- des premiers moyens de calcul pour produire un ou plusieurs défis $d \{dA, dB, \dots\}$ tels que $0 \leq dA \leq v - 1$,

20 - des deuxièmes moyens de calcul pour calculer, en fonction des réponses D reçues du dudit dispositif témoin et/ou dudit dispositif pilote, des engagements R' , en effectuant des opérations du type :

$$R' \equiv GA^{dA} \cdot GB^{dB} \cdot \dots D^v \bmod n$$

ou du type :

$$R' \cdot GA^{dA} \cdot GB^{dB} \cdot \dots \equiv D^v \bmod n$$

25 - des troisièmes moyens de calcul pour vérifier que les triplets $\{R', d, D\}$ sont cohérents.

33. Dispositif de contrôle selon la revendication 32 permettant de diminuer la charge de travail pendant une session destinée à vérifier l'authenticité d'une entité ;

dans le cas d'une authentification d'entité, le dispositif pilote est appelé dispositif démonstrateur,

pour prouver l'authenticité d'une entité ledit dispositif de contrôle exécute les étapes suivantes :

5 • **étape 1. engagement R du dispositif témoin :**

- le dispositif témoin produit au moins un engagement R à partir d'au moins une collection d'aléas $\{r_1, r_2, r_3, \dots\}$, telle que, pour chaque facteur premier p_i , chaque collection comporte un aléa r_i entier positif et plus petit que p_i , de telle sorte qu'il y a autant d'engagements R que de collections d'aléas ,

10 • **étape 2. défis produits par le dispositif contrôleur et destinés au dispositif témoin :**

- lesdits moyens de réception du dispositif de contrôle reçoivent tout ou partie de chaque engagement R , transmis par le dispositif démonstrateur, et le transmet au dispositif contrôleur,

15 - le dispositif contrôleur comporte des premiers moyens de calcul pour calculer, après avoir reçu tout ou partie de chaque engagement R , au moins une collection de défis d $\{dA, dB, \dots\}$ tels que $0 \leq dA \leq v - 1$, le nombre des collections de défis d étant égal au nombre d'engagements R , chaque collection $\{dA, dB, \dots\}$ comprenant un nombre de défis égal au nombre de paires de clés,

20 • **étape 3. réponse du dispositif témoin aux défis d :**

- ledit dispositif témoin comporte des quatrièmes moyens de calcul pour calculer des réponses D , à partir desdites collections de défis d $\{dA, dB, \dots\}$ reçues du dispositif contrôleur, de telle sorte qu'il y a autant de réponses D que d'engagements R et de défis d ,

25 • **étape 4. données destinées au dispositif contrôleur :**

- les moyens de réception du dispositif de contrôle reçoivent du dispositif démonstrateur chaque réponse D ,

 • **étape 5. vérification par le dispositif contrôleur :**

ledit dispositif contrôleur comporte des deuxièmes moyens de calcul pour calculer à partir de chaque réponse **D** un engagement **R'** en effectuant des opérations du type :

$$\mathbf{R'} \equiv \mathbf{GA}^{d_A} \cdot \mathbf{GB}^{d_B} \cdot \dots \mathbf{D'} \text{ mod } n$$

5 ou du type :

$$\mathbf{R'} \cdot \mathbf{GA}^{d_A} \cdot \mathbf{GB}^{d_B} \cdot \dots \equiv \mathbf{D'} \text{ mod } n$$

ledit dispositif contrôleur comporte des troisièmes moyens de calcul pour comparer et vérifier que chaque engagement reconstruit **R'** reproduit tout ou partie de chaque engagement **R** transmis à l'étape 2 par le dispositif démonstrateur

10

34. Dispositif de contrôle selon la revendication 32 permettant de diminuer la charge de travail pendant une session destinée à vérifier l'authenticité d'un message **m**,

dans le cas d'une authentification d'un message **m**, le dispositif pilote est appelé dispositif démonstrateur,

15

pour prouver l'authenticité d'un message **m**, ledit dispositif de contrôle exécute les étapes suivantes :

• étape 1. engagement **R** du dispositif témoin :

- le dispositif témoin produit au moins un engagement **R** à partir d'au moins une collection d'aléas $\{r_1, r_2, r_3, \dots\}$, telle que, pour chaque facteur premier p_i , chaque collection comporte un aléa r_i entier positif et plus petit que p_i , de telle sorte qu'il y a autant d'engagements **R** que de collections d'aléas ,

20

• étape 2. défis **d** produits par ledit dispositif contrôleur et destinés au dispositif témoin :

- lesdits moyens de réception du dispositif de contrôle reçoivent au moins un jeton **T** calculé et transmis par le dispositif démonstrateur en appliquant une fonction de hachage **f** ayant comme arguments le message **m** et chaque engagement **R**,

25

- ledit dispositif contrôleur comporte des premiers moyens de calcul pour

calculer, après avoir reçu le jeton T , au moins une collection de défis d $\{dA, dB, \dots\}$ tels que $0 \leq dA \leq v - 1$, le nombre des collections de défis d étant égal au nombre d'engagements R , chaque collection $\{dA, dB, \dots\}$ comprenant un nombre de défis égal au nombre de paires de clés,

5

• **étape 3. réponse du dispositif témoin au défi d :**

- ledit dispositif témoin comporte des quatrièmes moyens de calcul pour calculer des réponses D , à partir desdites collections de défis d $\{dA, dB, \dots\}$ reçues du dispositif contrôleur, de telle sorte qu'il y a autant de réponses D calculées par le témoin que d'engagements R et de défis d ,

10

• **étape 4. données destinées au dispositif contrôleur :**

- les moyens de réception du dispositif de contrôle reçoivent du dispositif démonstrateur chaque réponse D ,

• **étape 5. vérification par le dispositif contrôleur :**

ledit dispositif contrôleur comporte des deuxièmes moyens de calcul pour calculer à partir de chaque réponse D un engagement R' en effectuant des opérations du type :

15

$$R' \equiv GA^{dA} \cdot GB^{dB} \cdot \dots D' \bmod n$$

ou du type :

$$R' \cdot GA^{dA} \cdot GB^{dB} \cdot \dots \equiv D' \bmod n$$

20

ledit dispositif contrôleur comporte des troisièmes moyens de calcul pour calculer, en appliquant la fonction de hachage f ayant comme arguments le message m et chaque engagement R' , le jeton T' ,

ledit dispositif contrôleur comporte des quatrièmes moyens de calcul pour comparer et vérifier que le jeton T' est identique au jeton T transmis à l'étape 2 par le dispositif démonstrateur.

25

35. Dispositif de contrôle selon la revendication 32 permettant de diminuer la charge de travail pendant une session destinée à vérifier la signature numérique d'un message m ,

dans le cas d'une authentification d'un message m , le dispositif pilote est

appelé dispositif de signature,
pour prouver la signature numérique du message m , ledit dispositif de
contrôle exécute les étapes suivantes :

• **étape 1. engagement R du témoin :**

- 5 - le dispositif témoin produit au moins un engagement R à partir d'au moins
une collection d'aléas $\{r_1, r_2, r_3, \dots\}$, telle que pour chaque facteur premier
 p_i , chaque collection comporte un aléa r_i entier positif et plus petit que p_i ,
de telle sorte qu'il y a autant d'engagements R que de collections d'aléas ,

• **étape 2. défis d destinés au dispositif témoin :**

- 10 - ledit dispositif de signature calcule, en appliquant une fonction de hachage
 f ayant comme arguments le message m et chaque engagement R , au moins
une collection de défis d $\{dA, dB, \dots\}$ tels que $0 \leq dA \leq v - 1$, le nombre
des collections de défis d étant égal au nombre d'engagements R , chaque
collection $\{dA, dB, \dots\}$ comprenant un nombre de défis égal au nombre de
15 paires de clés,

- le dispositif de signature transmet les collections de défis d au
témoin,

• **étape 3. réponse du dispositif témoin au défi d :**

- 20 - ledit dispositif témoin comporte des quatrièmes moyens de calcul pour
calculer des réponses D , à partir desdites collections de défis d $\{dA, dB,$
 $\dots\}$, de telle sorte qu'il y a autant de réponses D calculées par le témoin que
d'engagements R et de défis d ,
- ledit dispositif témoin comporte des moyens de transmission pour
transmettre les réponses D au dispositif de signature et/ou au dispositif
25 contrôleur,

• **étape 4. données destinées au dispositif contrôleur :**

- les moyens de réception du dispositif de contrôle reçoivent du dispositif
de signature un message signé comprenant :

/ le message m ,

/ les collections de défis d ou les engagements R ,

/ chaque réponse D

• **étape 5. vérification par le dispositif contrôleur :**

cas où le dispositif contrôleur reçoit la collection des défis d ,

5 dans le cas où le dispositif contrôleur reçoit les collections des défis d et des réponses D ,

ledit dispositif contrôleur comporte

* des premiers moyens de calcul pour calculer à partir de chaque réponse D un engagement R' en effectuant des opérations du type :

$$10 \quad R' \equiv GA^{d^A} \cdot GB^{d^B} \cdot \dots D' \bmod n$$

ou du type :

$$R' \cdot GA^{d^A} \cdot GB^{d^B} \cdot \dots \equiv D' \bmod n$$

* des deuxièmes moyens de calcul pour calculer chaque défi d' , en appliquant la fonction de hachage f ayant comme arguments le message m et chaque engagement reconstruit R' ,

15

* des troisièmes moyens de calcul pour comparer et vérifier que chaque défi d' est identique au défi d figurant dans le message signé,

cas où le dispositif contrôleur reçoit la collection des engagements R

dans le cas où le dispositif contrôleur reçoit la collection des engagements

20

R et des réponses D ,

ledit dispositif contrôleur comporte

* des premiers moyens de calcul pour calculer chaque défi d' , en appliquant la fonction de hachage f ayant comme arguments le message m et chaque engagement R ,

25

* des deuxièmes moyens de calcul pour calculer alors la collection des engagements R' en effectuant des opérations du type

$$R' \equiv GA^{d^A} \cdot GB^{d^B} \cdot \dots D' \bmod n$$

ou du type :

$$R' \cdot GA^{d^A} \cdot GB^{d^B} \cdot \dots \equiv D' \bmod n$$

* des troisièmes moyens de calcul pour comparer et vérifier que chaque engagement R' reconstruit est identique à l'engagement R figurant dans le message signé.

36. Dispositif de contrôle selon l'une quelconque des revendications 31 à 35 tel que les composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, des clés privées QA, QB, \dots sont des nombres tirés au hasard à raison d'une composante QA_i, QB_i, \dots pour chacun desdits facteurs premiers p_i , lesdites clés privées QA, QB , pouvant être calculées à partir desdites composantes $QA_1, QA_2, \dots (QA_i, \dots)$, et $QB_1, QB_2, \dots (QB_i, \dots)$, ... par la méthode des restes chinois, ledit dispositif témoin comportant des moyens de calcul pour calculer lesdites clés publiques GA, GB, \dots ,

• en effectuant des opérations du type :

$$GA_i \equiv QA_i^v \bmod p_i$$

• puis en appliquant la méthode des restes chinois pour établir GA tel que

$$GA \equiv QA^v \bmod n$$

ou bien tel que

$$GA \cdot QA^v \bmod n \equiv 1$$

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer par les huitièmes moyens de calcul dudit dispositif témoin pour calculer chacun des GA_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

37. Dispositif de contrôle selon la revendication 36 tel que l'exposant public de vérification v est un nombre premier, de sorte que la paire de clés GA, QA confère une sécurité équivalente à la connaissance de la clé privée QA .

38. Dispositif de contrôle selon l'une quelconque des revendications 31 à 35 tel que l'exposant public de vérification v est du type

$$v = a^k$$

où k est un paramètre de sécurité plus grand que 1.

39. Dispositif de contrôle selon la revendication 38 tel que :

- l'exposant public de vérification v est du type

$$v = 2^k$$

où k est un paramètre de sécurité plus grand que 1,

- la clé publique GA est un carré gA^2 inférieur à n choisi de telle sorte que les deux équations

$$x^2 \equiv gA \pmod{n} \quad \text{et} \quad x^2 \equiv -gA \pmod{n}$$

n'ont pas de solution en x dans l'anneau des entiers modulo n

- ledit dispositif témoin comportant des neuvièmes moyens de calcul pour calculer les dites composantes $QA_1, QA_2, \dots (QA_i, \dots)$ de la clé privée QA en appliquant des formules telles que :

$$GA \equiv QA_i^{2 \exp(k)} \pmod{p_i}$$

ou bien telles que :

$$GA \cdot QA_i^{2 \exp(k)} \pmod{p_i} \equiv 1$$

et en extrayant la k ième racine carrée de GA dans le corps de Galois $CG(p_i)$

de sorte que le nombre d'opérations arithmétiques modulo p_i à effectuer par les neuvièmes moyens de calcul du dispositif témoin pour calculer chacun des QA_i pour chacun des p_i est réduit par rapport à ce qu'il serait si les opérations étaient effectuées modulo n ,

de sorte que la paire de clés GA, QA confère une sécurité équivalente à la connaissance de la factorisation de n .

40. Dispositif de contrôle selon la revendication 39 tel que pour extraire la k ième racine carrée de GA dans le corps de Galois $CG(p_i)$,

* dans le cas où le facteur premier p_i est congru à 3 modulo 4, les neuvièmes moyens de calcul du dispositif témoin appliquent notamment un algorithme du type :

$$x = (p+1)/4 ; y \equiv x^k \pmod{p-1} ; z = y ; QA_i \equiv GA^z \pmod{p_i}$$

* dans le cas où le facteur premier p_i est congru à 1 modulo 4, les neuvièmes moyens de calcul du dispositif témoin appliquent notamment un algorithme basé sur les suites de Lucas.

Par conséquent, le nombre : $x \equiv \frac{1}{2} v_{(p+1)/2} \pmod{p}$ est alors une solution à l'équation : $x^2 \equiv c \pmod{p}$.

Les relations suivantes sont utilisées pour calculer les suites $\{U\}$ et $\{V\}$ ensemble.

5 Pour doubler l'indice, $u_{2,i} = u_i \cdot v_i$; $v_{2,i} = v_i^2 - 2c^i$

Pour ajouter 1 à l'indice, $u_{i+1} = (S \cdot u_i + v_i)/2$; $v_{i+1} = (\Delta \cdot u_i + S \cdot v_i)/2$

La procédure suivante utilise trois variables : x pour u_i , y pour v_i et z pour c^i . L'indice cible est $(p+1)/2$; il est codé par une séquence de j bits. Cette séquence est examinée du bit de poids fort au bit de poids faible.

- 10 1. Donner à x la valeur 0 ; donner à y la valeur 2 ; donner à z la valeur 1.
2. Répéter j fois la séquence suivante.

Remplacer x par $x \cdot y \pmod{p}$.

Remplacer y par $y^2 - 2z \pmod{p}$

Remplacer z par $z^2 \pmod{p}$.

- 15 Si le j ième bit codant l'indice cible vaut 1, exécuter la séquence suivante.

Remplacer t par x .

Remplacer x par $(S \cdot t + y)/2 \pmod{p}$.

Remplacer y par $(S \cdot t + \Delta \cdot y)/2 \pmod{p}$

- 20 Remplacer z par $z \cdot c \pmod{p}$.

3. Remplacer y par $y/2 \pmod{p}$. Le résultat cherché est y .

2.2. Algorithme d'Euclide

L'algorithme d'Euclide opère la division des entiers. Soient deux entiers positifs x et y tels que x soit plus grand que y . Divisons x par y pour obtenir un quotient q positif et plus petit que ou égal à x et un reste r positif ou nul et plus petit que y .

Soit, $0 < y < x$

Par conséquent, $x = q \cdot y + r$ avec $0 < q \leq x$ et $0 \leq r < y$

2.2.1. Coefficients de Bezout et pgcd

This Page Blank (uspto)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☐ **FADED TEXT OR DRAWING**

☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☒ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

This Page Blank (uspto)